CYBER-SECURITY Sourcebook

WWW.DBTA.COM

Published by
Information Today, Inc.

Publisher of
database TRENDS AND APPLICATIONS
BDQ BIG DATA QUARTERLY

CYBERSECURITY SOURCEBOOK

From the publishers of database TRENDS AND APPLICATIONS BDQ BIG DATA QUARTERLY

PUBLISHED BY Unisphere Media—a Division of Information Today, Inc.

EDITORIAL & SALES OFFICE 121 Chanlon Road, New Providence, NJ 07974

CORPORATE HEADQUARTERS 143 Old Marlton Pike, Medford, NJ 08055

CYBERSECURITY SOURCEBOOK (ISBN: 2376-7383) is published annually by Information Today, Inc., 143 Old Marlton Pike, Medford, NJ 08055

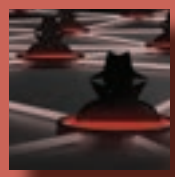
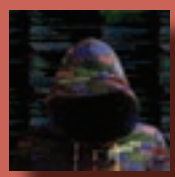
POSTMASTER
Send all address changes to:
Cybersecurity Sourcebook, 143 Old Marlton Pike, Medford, NJ 08055

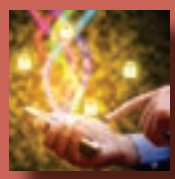
Cybersecurity Sourcebook is a resource for IT managers and professionals providing information on the enterprise and technology issues surrounding cybersecurity and the key challenges, opportunities, and technologies, as well as the approaches being evaluated, adopted, and bringing success. The *Cybersecurity Sourcebook* provides in-depth articles on the expanding range of cybersecurity technologies and best practices. Articles cover encryption and data masking, database auditing, database administration, IoT and connected devices, the business of data security, and regulatory compliance.

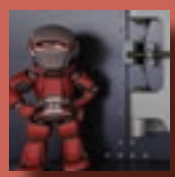
Information Today, Inc.

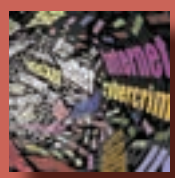
CYBERSECURITY SOURCEBOOK 2017

CONTENTS








Data Security Is Everyone's Job

By Joyce Wells

With data increasingly recognized as a highly valuable enterprise asset, data protection is understandably becoming a higher priority.

Today, the relentless stream of data breaches has elevated security as a concern. It's not just cybercriminals with nefarious intent that pose a threat, or even privileged users seeking to take advantage of their authority. Data breaches can happen in endless innocent ways—a conscientious employee sending assignments offsite to work on at home, a lost laptop or flash drive, or a click on a wrong file during a momentary lapse in judgment.

As a result, today, data security can no longer be considered strictly an IT responsibility. Today, data security is everyone's job.

And, as organizations collect more sensitive data than ever before that is stored in a greater variety of repositories—including NoSQL and big data platforms, on premise and in the cloud, and governed by regulations such as HIPAA Hitech, PCI, and the new EU GDPR—the stakes surrounding data management continue to rise. Financial penalties exist, but those may pale, experts say, compared to the potential loss of reputation and business opportunities.

Perimeter security is important, but that alone is not enough to ensure data protection. Instead, what is increasingly required is a holistic approach involving user education and an array of solutions such as encryption, monitoring and auditing, automation, and identity management.

To explore the issues surrounding data protection, including the role of people, processes, and technology in creating a proactive security stance, *Database Trends and Applications* is introducing the *Cybersecurity Sourcebook*. This special report contains articles penned by subject matter experts on the full range of data security issues facing enterprise data professionals and the approaches that can help.

Plan now for preventing and handling a breach, they advise. The question is not "if" it will occur, but "when." ■

ORACLE®

Finding a Cloud Partner You Can Trust

Trust is paramount in choosing a cloud partner—not just for your own data, but also for the data owned by your end-customers. According to a report from the Economist Intelligence Unit, 92 percent of executives say their customers are willing to share personal information such as name, contact information, and demographic details with their trusted vendors.

Maintaining customer data is a huge responsibility, especially when you consider the consequences of errors, omissions, and breaches—which can involve losing face with customers and millions of dollars in fines. Keep that in mind whenever you decide to do business with a cloud service provider. You are entrusting it with your data plus whatever customer data passes through your system.

Service provider contracts should not only stipulate terms for capacity, availability, and performance. They should also give you peace of mind. More and more, that peace of mind stems from unwavering confidence in the security of your applications and data. Verifying the security capabilities of your cloud vendor includes having transparency into how it secures its cloud environment. You should have a clear understanding of roles and responsibilities for system access, and visibility into security audits from a trusted third party.

Unfortunately, most customers have only a vague understanding of what their cloud providers do or don't do to protect their data. In a survey conducted by the Independent Oracle Users Group, 58 percent of respondents admitted that they don't know whether their cloud providers are accessing their data, and only 38 percent said their providers will notify them of security breaches. Worse still, only one in four respondents to the survey said they have received assurances that their data will be expunged after the contract with the cloud provider ends.

Oracle Cloud customers can receive periodically published audit reports by Oracle's third-party auditors. Customers may request a copy of the current published audit report available for a particular Oracle Cloud service. Administrative access to your Oracle Cloud environment includes multiple security zones to restrict access on a "need to know" basis for all IT staff. Logical access controls encrypt data on staff computers, along with personal firewalls, two-factor authentication, and role-based accounts.

Oracle offers preventive security controls for data at rest and in transit, including encryption by default as part of Oracle Database Cloud Service, redaction of sensitive application-layer data, restriction of privileged-user capabilities, subsetting/masking of data in nonproduction environments, and monitoring of user activities.

BUILDING ORACLE'S DEFENSE-IN-DEPTH STRATEGY

Oracle Cloud is built around multiple layers of security and multiple levels of defense throughout the technology stack, from the application layer clear down to the silicon layer. Redundant controls provide exceptional resiliency in the event of a security breach. If a vulnerability is discovered and exploited in one layer, the attacker will invariably confront another security control in the next layer. But having the world's best security technology is only part of the story. Oracle aligns people, processes, and technology to offer an integrated defense-in-depth platform.

- **Preventive** controls mitigate unauthorized access to sensitive systems and data
- **Detective** controls reveal unauthorized system and data changes through auditing, monitoring, and reporting
- **Administrative** measures address security policies, practices, and procedures

BRINGING INTELLIGENCE TO THE SOC

Traditional security operations centers (SOCs) protect applications and users via static "prevent and defend" tactics. They keep bad guys out of the network, but they don't adapt contextually to the prospect of an attacker getting into the network. They protect the corporate network, but not the applications and data residing in the cloud. That's a problem for companies with hybrid cloud strategies.

Oracle offers customers a more intelligent alternative that **prevents** probable threats, **detects** threats that get through, **responds** to those threats, and gathers intelligence to **predict** potential threats before they occur—all based on the **context** of user events, moment-to-moment. **Oracle Identity Security Operations Center** solution is a cloud-based, context-aware, intelligent automation service that can detect and respond to advanced threats and persistent attacks as well as establish a feedback loop for adaptation and evolution. It protects users, applications, APIs, content, and workloads. ■

ORACLE
www.oracle.com

Cautionary Tales From Data Breach Headlines

While there is an impressive assortment of security solutions on today's market, technology alone is inadequate for addressing the overwhelming amount of threats on the horizon.

By Joe McKendrick

Regardless of your political persuasion, the infamous hacking of the Democratic National Committee internal emails was a wake-up call on the necessity of corporate vigilance, combined with end-user education and awareness. According to the FBI and U.S. Department of Homeland Security, the perpetrators gained access to the DNC's servers through targeted spear-phishing campaigns, in which they tricked targeted users into clicking bogus links that either deployed malware or directed them to a fake webmail domain. The intruders were then able to harvest credentials to gain access and steal sensitive email content.

Unfortunately, the high-profile election season data theft was only one of countless incidents seen across government, corporate, and nonprofit organizations throughout the globe. The hackers—be they state actors, political activists, or just plain criminals—are out there, and what they're banking on is not their abilities to ram their way into well-hardened corporate systems, but rather their ability to exploit weak spots—vulnerabilities such as lack of end-user awareness or mistakes or corporate laxity.

Adding to the challenge is the continuing threat from inside data breaches, both intentional and unintentional. Disgruntled employees, or individuals tempted by compensation from nefarious outside parties may put sensitive corporate or customer data at risk. There's also a great deal of inherent risk in the mishandling of sensitive data that hasn't been subject to safeguards such as encryption or de-identification. Such incidents may be outside the domain of a well-protected data center, as many breaches occur at the hands of contractors or business partners.

The unending stream of bad news about data breaches doesn't appear to be showing any signs of letting up soon. According to PrivacyRights.org, which keeps a running tally of the latest public acknowledgments by organizations of data breaches, the nature of the breaches reflect both attacks from outside parties, as well as issues stemming from neglect or mistakes made inside organizations.

- Centene, a health insurance company, lost track of six hard drives that contained protected health information of approximately 950,000 patients, including names, addresses, birth dates, Social Security numbers, member ID numbers, and health information. The company realized the drives were missing in an audit of its IT assets.
- Western Union reported a breach of personal customer data, including drivers'

licenses, Social Security numbers, and birthdates, as a result of a hacking of a vendor-supplied external system formerly used by Western Union for secure data storage.

- Los Angeles County was subject to a phishing email attack that affected approximately 108 out of 120,000 county employee email accounts, which may have compromised email account usernames and passwords by appearing to come from a trustworthy source. Information at risk included names, birthdates, Social Security numbers, drivers' licenses, state identification numbers, payment card information, bank account information, home addresses, phone numbers, and medical information.
- Personal data for 134,000 U.S. Navy sailors in a re-enlistment approval database was stolen from a contractor's laptop. Data included names and Social Security numbers of service members.
- Internal Revenue Service employees sent unencrypted emails which contained 8,031 different taxpayers' personally identifiable information. Investigators found 326 unencrypted emails containing taxpayer data. At least 275 of the emails were sent internally within IRS, while 51 emails were sent outside of the agency's network to non-IRS email accounts. Of those emails sent externally, 20 were sent to six IRS employees' personal email accounts.

These are just a few examples of various breaches reported over the past year—and the list goes on and on. The job of locking down and securing data just keeps getting harder, and various forces shaping the enterprise data space are adding to the complexity. More business is online, and therefore, many systems are touching the internet. New data platforms for data processing and management and storage, such as Hadoop, NoSQL, and cloud, are adding a level of complexity to security for data infrastructure that was never a consideration in the more orderly relational era.

*One of the challenges with data security is the **widespread perception** that it is primarily an IT concern.*

Next, add in cloud computing—the biggest wave sweeping through the information technology space—to today's mix of security concerns. Interestingly, cloud is reshaping perceptions of security in divergent ways. There's the long-standing fear of entrusting data security to outside cloud providers, which has made executives and IT managers nervous about moving to cloud computing. At the same time, however, there's a growing acknowledgment that cloud-based providers offer greater data security than organizations are capable of managing within their own data centers. A survey of 306 IT professionals conducted by Unisphere Research, a division of Information Today, Inc., finds growing interest in moving data to the cloud, despite security concerns. In fact, nearly half of the respondents, 48%, feel that moving data to a public cloud will provide better security than can be achieved on premises ("Perspectives from Leading IT Professionals: 2016 IOUG Cloud Security Survey," September 2016).

Beyond cloud, the complexity of today's environments also lends itself to data breaches. A survey of 3,000 chief security officers by Cisco cites "budget constraints, poor compatibility of systems, and a lack of trained talent as the biggest barriers to advancing their security postures." There may even be too many security solutions, making things even more complicated to manage. As the Cisco survey found, chief security officers also believe that their security departments are increasingly complex environments, with 65% of organizations using from six to more than 50 security products, adding to the potential for security effectiveness gaps.

While there is a great deal of technology being employed to lock things down, there is still a need for user awareness and education. The Cisco survey found criminals leading a resurgence of classic attack modes, such as adware and email spam, the latter at levels not seen since 2010. Spam accounts for nearly two-thirds (65%) of email—with 8% to 10% classified as malicious. Global spam volume is rising, often spread by large and thriving botnets.

There's a significant cost to the data breaches that organizations have been suffering over the past year. The most recent study by IBM Security and Ponemon Institute, covering 400 enterprises, found that the average cost of a data breach for companies surveyed has grown to $4 million, representing a 29% increase of such costs since 2013. As these threats become more complex, the cost to companies continues to rise. In fact, the study found that companies lose $158 per compromised record. Breaches in highly regulated industries were even more costly, with healthcare reaching $355 per record—a full $100 more than in 2013. In addition, cybersecurity incidents continue to grow in both volume and sophistication, rising 64% annually.

Much of this cost comes out of lost business, industry research confirms. For example, the Cisco study found that 22% of breached organizations lost customers—40% of them lost more than 20% of their customer base. In addition, 29% lost revenue, with 38% of that group losing more than 20% of revenue. Twenty-three percent of breached organizations lost business opportunities, with 42% of them losing more than 20%.

Addressing the Challenge

How can organizations address this challenge? While there is an impressive assortment of security solutions in today's market, technology alone is inadequate for addressing the overwhelming amount of threats on the horizon.

Develop a holistic approach. Technology solutions—such as automation, encryption, and identity management—may be effective in hardening systems

*Recent high-profile data breaches reflect both **attacks from outside parties**, as well as issues stemming from neglect or mistakes made inside organizations.*

and patching potential weaknesses in data-transfer areas, but there's an even stronger need to increase end-user engagement in the process. The ability to effectively deal with data security issues—from prevention to detection to remediation—requires a combination of planning, education, and speed. A holistic security strategy that incorporates people, process, and technology is the best line of defense against the impact of data breaches. The burgeoning complex web of technology, along with the overwhelming number of security alerts, "is a recipe for less, not more, protection," the Cisco report states.

Elevate security to the business. One of the challenges with data security is the widespread perception that it is primarily an IT concern. The authors of the Cisco report urge that enterprises "make security a business priority: Executive leadership must own and evangelize security and fund it as a priority." In addition, operational discipline is key, the report's authors add. "Review security practices, patch, and control access points to network systems, applications, functions, and data." Adopt an integrated defense approach, the Cisco authors also advocate. "Make integration and automation high on the list of assessment criteria to increase visibility, streamline interoperability, and reduce the time to detect and stop attacks. Security teams then can focus on investigating and resolving true threats."

Have a plan. The IBM-Ponemon study found companies that had predefined business continuity management processes in place found and contained breaches more quickly, discovering breaches 52 days earlier and containing them 36 days faster than companies without such processes. "The process of responding to a breach is extremely complex and time consuming if not properly planned for. Amongst the required activities, a company must work with IT or outside security experts to quickly identify the source of the breach and stop any more data leakage," the report's authors advise.

Communicate as early and often as possible. Communication with customers, partners, and stakeholders is also essential. In many localities, such public communication is mandated (and is the source of many of the reports seen in PrivacyRights.org, cited earlier in this article).

Consumers understand that hacking incidents and data breaches do occur, but the essential point is how organizations react once an incident takes place. Is management forthright and ready to work with affected individuals? It's also important to note that adequately addressing data breach incidents also requires an investment of time, money, and resources on the part of affected organizations. Dealing with the aftermath of a data breach "takes countless hours of commitment from staff members, taking time away from their normal responsibilities and wasting valuable human resources to the business," the IBM-Ponemon report states. "Incident response teams can expedite and streamline the process of responding to a breach, as they're experts on what companies need to do once they realize they've been compromised. These teams address all aspects of the security operations and response lifecycle, from helping resolve the incident, to satisfying key industry concerns and regulatory mandates. Additionally, incident response technologies can automate this process to further speed efficiency and response time."

Hold cloud providers' feet to the fire on security. There is a need to balance security with transparency and access, as found in the Unisphere-IOUG research. Nearly one-third of respondents expect to experience some type of data breach within their cloud environments over the coming year. Potentially, public cloud services may offer greater protection than enterprise data centers are capable of delivering, and close to half of enterprise data managers agree. However, cloud providers are not yet stepping up to this opportunity. Most of the professionals in this survey say they do not have assurances that their public cloud providers are doing enough to protect their data.

Monitor and audit on an ongoing basis. Many organizations engage in real-time monitoring of activities across their data environments, which helps ensure that administrators are alerted to major breaches as they happen. There are many instances, however, in which malware or other malicious hacks are occurring for days, weeks, and even months before they are discovered. Regular audits of data usage may uncover irregularities or suspicious activities, but if these audits only occur periodically, there is potential for mischief for extended time periods. ■

Joe McKendrick is an author and independent researcher covering innovation, information technology trends, and markets. Much of his research work is in conjunction with Unisphere Research, a division of Information Today, Inc. (ITI), for user groups including SHARE, the Oracle Applications Users Group, and the Independent Oracle Users Group. He is also a regular contributor to *Database Trends and Applications*, published by ITI.

THE MOST ADVANCED APPLICATION & DATA SECURITY PLATFORM

MENTIS

DISCOVERY | MASKING | ENCRYPTION | TOKENIZATION | MONITORING | RETIREMENT

BUILT ON A CLOUD-READY, ENTERPRISE-CLASS SINGLE PLATFORM

"The discovery capabilities offered by Mentis are excellent, and market leading."
– Leading Analyst Firm, 2017

"The company offers a number of unique or near unique features such as location-based, conditional masking and time slice based subsetting. Its iRetire product will be especially beneficial in regulated environments such as the EU's GDPR (General Data Protection Regulation)."
– Leading Analyst Firm, 2017

"The company's offering (which also includes iMonitor and iProtect) is much broader in scope than most of its competitors. Only one other company could offer something comparable but that would be in diverse products that are not well integrated."
– Leading Analyst Firm, 2017

"MENTIS goes further, in our opinion, than any other supplier in its facilities for discovering sensitive data."
– Leading Analyst Firm, 2017

"It is the first company, as far as we know, to introduce conditional masking based on location."
– Leading Analyst Firm, 2015

"In 17 years working on this system, no way I could have known that."
– iDiscover™ customer on the surprising volume of sensitive data that they did not know was in their system, 2016

"MENTIS is one of four vendors to provide a comprehensive solution."
– Leading Analyst Firm, 2017

3 Columbus Circle . 15th Floor . New York, NY . 10019 - 800 267 0858

wwww.mentisoftware.com

The Role of the DBA in Cybersecurity

For data security, DBAs are the technology experts who translate the specific requirements as outlined by the business into an actual implementation.

By Craig S. Mullins

Protecting sensitive data from criminals, hackers, and other prying eyes is an important aspect of providing security for modern systems and applications. Data is central to business, and whenever it is breached for any reason, there will be repercussions, whether they be financial, regulatory, or otherwise. And, the most important data is stored in a database management system. As such, database administrators are tasked with protecting the core data assets of their organizations.

Current State of Data Security

Data security and privacy are top corporate initiatives these days. Instead of being ignored and relegated to IT staff as in the past, today, executives are being held accountable for data protection. This change has been driven, in many cases, by regulatory requirements, but also as a reaction to the publicity and negative impact of the ever-increasing number of data breaches. This shift has elevated data security and protection planning to the executive level.

Of course, executives are not the implementers. For data security, DBAs are the technology experts who translate the specific requirements as outlined by the business into an actual implementation. But having executives involved with—and held accountable for—data security makes it easier for the DBA team to get visibility and funding for data security projects.

Furthermore, implementing security measures within IT systems has a more elevated status in organizations because customers are becoming increasingly suspicious of big companies in terms of what data is being collected and how businesses secure and protect their data. Most organizations could use improved techniques and tools for protecting data, and the big data trend only exacerbates the situation. Organizations must be able to quantify the business value of their data and categorize exposure and loss of data in terms of issues such as the reduction in value, impact to the company's reputation, and loss of potential trade secrets.

Fortunately, DBMSs have gained more security features over the past few years and will continue to do so. Database security is much more than simple logon/password authentication and authorization, but now comprises multiple additional techniques and capabilities.

Improving Database Systems Security

An important database security feature for data protection is ***data encryption***. When data is encrypted, it is transformed

DATA IS EVERYWHERE. PUT IT TO WORK FOR YOU.

DBTA magazine delivers advanced trends, analysis, and case studies serving the IT and business stakeholders of complex data environments. Each issue is jam-packed with everything you need to know about data and information management, big data, and data science. Stay informed and up-to-date on the industry with content that is original, factual, and valuable.

Don't miss another issue. Learn to make data work for you!

database
TRENDS AND APPLICATIONS

Subscribe FREE* today!

**Print edition free to qualified U.S. subscribers.*

dbta.com/subscribe

using an algorithm to make it unreadable to anyone without the decryption key. The general idea is to make the effort of decrypting so difficult as to outweigh the advantage to a hacker of accessing the unauthorized data. There are two situations where data encryption can be deployed: data in transit and data at rest. In a database context, data "at rest" encryption protects data stored in the database, whereas data "in transit" encryption is used for data being transferred over a network.

Encrypting data at rest is undertaken to prohibit "behind-the-scenes" snooping for information. When the data at rest is encrypted, even if a hacker surreptitiously gains access to the data behind the scenes, without the decryption key, the data is meaningless. Data at rest encryption most commonly is supported by using built-in functions, a DBMS feature, such as Oracle Transparent Data Encryption, or through an add-on encryption product.

Encrypting data in transit protects against network packet sniffing. If the data is encrypted before it is sent over the network and decrypted upon receipt at its destination, it is protected along its journey. Anyone nefariously attempting to access the data en route will receive only encrypted data. And again, without the decryption key, the data cannot be deciphered. Data-in-transit encryption most commonly is supported using DBMS system parameters and commands or through an add-on encryption product.

A growing number of DBMSs offer ***label-based access control (LBAC)***, which delivers a lower level of control over authorization to specific data in the database. With LBAC, it is possible to support applications that need a more granular security scheme. LBAC can be set up to specify who can read and modify data in individual rows and/or columns.

LBAC is not for every application; it is geared more for top secret, governmental, and similar types of data. For example, you might want to set up an authorization scenario such that each column and row have specific rules pertaining to which employees can see and manipulate the data. Setting up such a security scheme is virtually impossible without LBAC. An administrator configures the LBAC system by creating security label components, which are database objects used to represent the conditions determining whether a user can access a piece of data. A security policy, composed of one or more security label components, is used to describe the criteria for determining who has access to what data. The security administrator defines the policy by creating security labels that are composed of security label components. Once created, a security label can be associated with individual columns and rows in a table to protect the data held there. When a user tries to access protected data, that user's security label is compared to the security label protecting the data.

*The DBA should be an **advisor** to the business in terms of the types of **database security** that can be enabled.*

Any attempted access to a protected column will fail when the LBAC credentials do not permit that access. If users try to read protected rows not allowed by their LBAC credentials, the DBMS simply acts as if those rows do not exist. This is important because sometimes even having knowledge that the data exists (without being able to access it) must be protected.

Consult your DBMS documentation for where and how to establish this hierarchy and how to use LBAC.

An additional technique for protecting database data is to deploy ***data masking and obfuscation***. Data masking is the process of protecting sensitive information in databases from inappropriate visibility by replacing it with gibberish or realistic but not real data (in the case of production data used in test systems). The goal is that sensitive, personally identifiable information is not available outside of the authorized environment. Protecting sensitive data using data masking can prevent fraud, identity theft, and other types of criminal activities. A common usage of data masking is to comply with PCI-DSS regulations to show only the last 4 digits of a payment card number on a receipt.

Data masking can be done while provisioning test environments so that copies created to support application development and testing do not expose sensitive information. Valid production data is replaced with usable, referentially intact, but incorrect or obfuscated data. After masking, the test data is usable just like production data, but the information content is secure.

It is possible to mask data using a variety of techniques. A good data masking solution should offer the ability to mask using multiple techniques. Common techniques include substitution, shuffling, number and data variance, nulling out, encryption, and table-to-table synchronization. Data masking is supported by many DBMS offerings as well as by third-party products.

Yet another useful technique available in some DBMS products is the concept of a ***trusted context***. A trusted context is used to identify a specific location from which interactions between the DBMS and an application are authorized. This establishes a trusted relationship between the DBMS and an external entity, such as a middleware server. Without a trusted context,

IRI DATA PROTECTOR SUITE

The Questions Stop Here.

- Find, classify, and protect PII and other sensitive data
- Comply with domestic and international privacy laws
- Award-winning data security you can afford

IRI
The CoSort Company

Innovative Routines International (IRI), Inc.

www.iri.com/products/iri-data-protector

*DBMSs have gained **more security features** over the past few years and will continue to do so.*

connecting to these tiered platforms uses one system userid for establishing the connection, as well as for performing all transactions on behalf of every end user. That means that even though individual users authenticate at the application server, the application itself uses a generic authid and password, perhaps hard-coded into programs. The generic authid has the authority to access and modify data in application tables, which can cause problems if the password becomes common knowledge.

A trusted context solves this problem by granting the privileges for dynamic SQL activity to a ROLE, instead of to a general authid. The ROLE, available only within the trusted context, provides context dependent privileges. The privileges granted to the ROLE can be exercised only through the trusted connection.

Database auditing, sometimes referred to as data access monitoring (DAM), is yet another data protection technique that is growing in adoption. Database auditing is the process of monitoring access to and modification of selected database objects and resources within operational databases and retaining a detailed record of the access that can be used to proactively trigger actions and can be retrieved and analyzed as needed.

Sensitive corporate data cannot be fully protected by simply setting up database authorization using the controls within the database software. This is so because it is not possible to guarantee that surreptitious access to sensitive data is blocked with simple database authorization mechanisms. And secondly, it is possible for authorized users to nefariously access data. Database auditing can help protect data in both of these situations.

All of the major RDBMS products offer built-in capabilities for auditing databases, but ISVs offer more capable software with more flexible capture technology, prepackaged compliance reports, and multi-DBMS support. Database auditing software can comprehensively track the usage of database resources and authority. When auditing is enabled, each database operation produces a detailed audit trail of information, tracking what data was accessed, who accessed it, and when. Operators can analyze the audit trail and generate reports showing access and modification patterns against the sensitive data in the DBMS.

Database auditing helps answer questions such as, "Who accessed the payment account details for Mr. Jones?" or, "When was Mrs. Smith's appointment time changed?" as well as, "Who changed that appointment time?" It is even possible to answer more detailed questions such as, "What was the old appointment time prior to the change?"

Of course, database auditing can create management issues. First, we have the need for separation of duties, which means that audited individuals should not be involved in managing the audit process. But DBAs typically control the starting and stopping of audit traces. What is to prevent a DBA with hacking on his mind from stopping the audit trace? Implementing privileged user auditing can manage this issue.

Another problematic area is performance management. One of the long-standing issues with such approaches is the large amount of resources that auditing can consume. When auditing is enabled, it can slow down database performance. But if you tackle the task appropriately, by pinpointing who and what needs to be audited—and possibly using advanced software to minimize the overhead—performance issues can be mitigated.

Unfortunately, even though all of these features are commonly available in many of the most popular RDBMSs, their adoption has not been as widespread as is needed. Time is required for DBAs to learn and implement new and advanced security options, and this is the current state of database security in most shops.

*Although **data protection features** are commonly available in many of the most popular RDBMSs, their **adoption has not been** as widespread as is needed.*

The Role of the DBA

Most DBAs have significant IT experience and have worked their way into a trusted position as a DBA. Nevertheless, DBAs are a significant insider threat in most organizations because they have elevated authority to access data and make changes to database structures. DBAs are, for the most part, trustworthy and want to do a good job in terms of managing and protecting their company's data. But there are always exceptions (see http://www.computerworld.com/s/article/298312/Rogue_DBA_Steals_Sells_Personal_Info),

and that is why one of the most common forms of database auditing implemented today is privileged user auditing.

DBAs, typically with high-level authority such as DBADM or SYSADM privileges, may have carte blanche access to the database instance and all its data. DBAs are trusted agents and should not abuse the overarching privileges they are granted. The general maxim of "trust but verify" applies in this case. DBAs need a high degree of authorization to do their job, but that also brings the opportunity for nefarious activity. Implementing privileged user auditing to track every action taken by such users is a wise course of action. Using a database auditing solution to enforce privileged user tracking can ensure that trusted users are acting appropriately.

The DBA should be an advisor to the business in terms of the types of database security that can be enabled. At a high level, this boils down to being able to answer four questions—Who is it? (authentication); Who can do it? (authorization); Who can see it? (encryption); and Who did it? (audit)—and ensuring that these issues are dealt with technologically in the DBMS. DBAs are not required to understand business-specific regulatory requirements, but must be able to understand the regulations that are communicated to them and translate that into actual DBMS functionality, if it exists, to satisfy the requirement.

The Future

The near-term future must be spent on understanding and implementing the database security and protection measures that are already available to us. As we make progress there, the next step is to protect more types of data and to make more use of autonomics and analytics.

In terms of more types of data, it is not just relational data but also data in NoSQL databases and big data platforms that is becoming more common, that also need to be protected. In many cases, security is often an afterthought, if it is thought of at all, in many of these systems. As more types of non-relational data stores get implemented, integration of security methods and protocols across disparate, heterogeneous DBMSs will need to be implemented. Administering security separately for each DBMS in use (e.g., Oracle, SQL Server, MongoDB, and Cassandra) will be burdensome, and overarching techniques will be desired.

*In terms of **more types of data**, it is not just relational data but also data in NoSQL databases and big data platforms, which are becoming more common, that also **need to be protected**.*

Higher transaction velocities will result in more real-time event processing. This can have a profound impact on data protection and security. For example, fraud detection benefits from being as close to real time as possible in order to perhaps become fraud prevention. And real-time processing of large data streams is another aspect of big data projects that is likely to be a challenge for DBAs.

But keep in mind that big data projects typically are accompanied by powerful predictive analytics. By analyzing reams of data and uncovering patterns, intelligent algorithms can make reasonably solid predictions about what will occur in the future. This requires being adept enough to uncover the patterns before changes occur, but not necessarily in real time. An expert system that recognizes data access patterns can have a big impact on improving data protection procedures. More usage of and reliance on AI and machine learning capabilities will bolster our ability to protect corporate data. These improved threat detection capabilities will be able to recognize patterns of attack on data and stop them automatically—before your data has been compromised.

The bottom line though is that there will be an ever-increasing number of threats to our databases. Why is that so? Well, it is like the old saying goes: "Why did you rob that bank? Because that's where the money is!" Hackers will target databases because that is where the data is. That means that we need to be diligent in implementing the security measures currently at our disposal to stop the current onslaught of potential hacking, but also be prepared to implement new and improved database security methods and procedures as they become available. ■

Craig S. Mullins is president and principal consultant with Mullins Consulting, Inc. He has over 3 decades of experience in all facets of data management and database systems development. Mullins is the author of two books: *DB2 Developer's Guide* and *Database Administration: The Complete Guide to Practices & Procedures*. Mullins is also an IBM Champion for Analytics, a DB2 Gold Consultant, and a member of the IDUG Volunteer Hall of Fame. You can reach him via his website at www.MullinsConsulting.com.

Getting Ready for GDPR

A metadata-driven approach is important for ensuring compliance with the EU's new data privacy law.

By Mika Javanainen

One of the biggest challenges IT professionals responsible for corporate data will face in 2017 comes from a law passed by the European Union due to take effect in 2018, the General Data Protection Regulation (GDPR).

The GDPR is intended to better protect the personal information of European citizens, and it comes with stiff penalties for companies that don't comply. It is also far-reaching in nature, as it applies not to just EU member countries, but also organizations outside the EU that collect personal data on EU citizens. That means a U.S.-based company that sells goods or services to an EU citizen, and during this process collects their personal data, will be subject to GDPR requirements for data privacy and protection.

While the GDPR spells out in no uncertain terms the level of protection companies must provide for personal data, it says little about which technologies organizations can use to deliver those protections. One approach companies would do well to consider is an enterprise content management (ECM) system that leverages metadata to enforce strict controls and security measures to protect personal customer information.

GDPR Explained

GDPR essentially replaces the EU's Data Protection Directive, which was adopted in 1995. Scheduled to take effect in May 2018, the GDPR is intended to provide EU citizens with a number of benefits, including easier access to their personal information housed by any company that collects it, as well as details about how the company uses their data. It also gives citizens a right to data portability, such as when they switch service providers, and the right to have their data deleted. In addition, it gives citizens the right to know when their data has been compromised, through a provision that requires companies to alert authorities within 72 hours of any data breach involving personal data.

For businesses that must comply with GDPR, the updated regulation promises to simplify existing rules and guidelines. Rather than trying to adhere to a patchwork of data privacy rules country by country, the GDPR will be a single law that applies to companies operating within any EU county. The European Commission estimates this will save companies around 2.3 billion euros a year by doing away with "the current fragmentation and costly administrative burdens."

Perhaps the biggest change that GDPR brings is in terms of jurisdiction. Previously there was some ambiguity about the extent to which the EU's Data Protection Directive applied to companies based outside of the EU. The GDPR clears that up, saying "it applies to all companies processing the personal data of data subjects residing in the Union, regardless of the company's location." The law makes it incumbent upon any company that collects personally identifiable information (PII) on EU citizens to meet GDPR requirements.

GDPR Requirements and Penalties for Non-Compliance

As spelled out in the summary of articles on the GDPR website, requirements include adhering to the theme of "privacy by design," which calls for the inclusion of data protection from the onset of system design. The regulation calls for "appropriate" technical and organizational measures to meet this requirement. It includes the concept of "data minimization," meaning holding only data that's absolutely necessary to the purpose at hand and limiting access to PII to those "needing to act out the processing."

The GDPR also requires companies to perform data protection impact assessments (DPIAs) to identify any risks of noncompliance, so the company can take steps to address them.

Public authorities and companies that process PII for 5,000 or more individuals in any 12-month period must also appoint a data protection officer (DPO). This individual must have expert knowledge of data protection laws and practices and be responsible for ensuring the company is in compliance.

Companies are also responsible for ensuring any "sub-processors" they hire to help manage or process PII are also in compliance with the GDPR. That may apply to not only third-party data processing companies, but any supply chain partners with which a company needs to share customer PII.

As mentioned above, the regulation also requires companies to report any security breaches that are likely to involve compromise of PII within 72 hours of learning of the breach. However, the GDPR does not require notification of a breach for data that is encrypted or "otherwise protected."

Companies will face stiff penalties for not adhering to the GDPR, with fines of up to 20 million euros (about $21 million) or 4% of annual revenue, whichever is larger, for the most egregious offenses.

And while its intent and requirements are clear, the law makes no mention of which technologies or specific processes companies must employ to meet those requirements, providing only general guidelines. That means individual companies are left to devise their own plans for ensuring compliance with the GDPR.

ECM, Metadata, and GDPR Compliance

At its core, the GDPR is all about protecting content—more specifically, personal information about individuals. With this in mind, it stands to reason that an ECM system, particularly a metadata-based ECM solution, can play a pivotal role in helping companies comply with the GDPR.

Metadata, often described as "data about data," generally takes the form of attributes that describe the data file or object. A Word document, for example, will include metadata that denotes its file type, size, author, date created, and date modified, all of which are important data points that help individuals quickly find and access specific documents and information objects.

A metadata-driven ECM solution enables companies to add more descriptive tags that are useful from a content management perspective and for ensuring compliance with laws such as GDPR.

Consider the most basic task associated with GDPR: identifying files or objects that contain PII. Some of this can be done using text analytics tools and by applying metadata for the records. Moreover, the ability to manually tag PII data is important because some PII data is stored in file formats such as images that cannot be analyzed and indexed as well as text documents.

Additionally, certain categories of files can be treated as PII by default. Contracts and invoices, for example, by their nature contain sensitive customer information that should be protected. So, within the ECM system, any file labeled "contract" or "invoice" would be treated as PII. More importantly, it is crucial to determine the person whose data is in the file since citizens can now request companies to provide an index of the PII data that the company stores about them.

Once it's determined that a given file or object contains PII, the next challenge is ensuring it is treated as such. Here again, a metadata-driven ECM system can play a key role by automating what happens to this class of information.

This can take several forms. For starters, a company may determine that all PII should be properly encrypted both in transit and at rest and that it should be purged as soon as possible after the mandatory retention period for the data passes. These policies help companies mitigate the risks of data breaches and therefore better protect customers' data sovereignty. While all data in an ECM system should be encrypted, applying data destruction policies is a more complex task because there are numerous types of records with different retention policies. Modern ECM solutions can ease this task by providing a dynamic way to manage records with metadata-driven file plans.

A metadata-based ECM solution will also support automated access control and permissions management capabilities to ensure compliance with the GDPR requirement that only those who need to act on data should have access to it. Organizations can set access permissions that apply to entire classes of documents—such as "invoices" for files that have been assigned a "customer data" metadata attribute—and enforce access controls that provide different levels of access to various users or groups of users. The finance manager, for example, may be able to view any invoice while financial analysts assigned to certain regions are allowed to view only invoices from companies within those regions.

A key benefit to this kind of setup is that it's relatively easy to manage because it's based on employee roles, not individuals. If the finance manager leaves or moves to a different position, a simple title change in the corporate user directory is all that's required to change access rights within the ECM system.

Similarly, a metadata-driven ECM system can help companies ensure they are storing PII appropriately. For example, the GDPR says companies shouldn't keep PII for longer than is necessary.

Get Your GDPR House in Order

Whether viewed as a welcome remedy for the tangled web of country-by-country laws on personal data or just another onerous regulation that must be followed, the GDPR is the law of the land in the EU— and far beyond. Given the stringent penalties for non-compliance, organizations must take stock of their current data protection strategies and practices, and ensure they are taking appropriate steps to protect PII. ■

Mika Javanainen is vice president of product management at M-Files Corp. He is in charge of managing and developing M-Files' product portfolio, roadmaps, and pricing globally. Prior to his executive roles, Javanainen worked as a systems specialist, where he integrated document management systems with ERP and CRM applications. A published author, Javanainen has an executive MBA in International Business and Marketing. Follow him on Twitter at @mikajava.

Stay connected.

Database Trends and Applications reports on big data, analytics, data science, business intelligence and all aspects of data creation, management, and storage. Connect with us and get industry news, trends, and analysis, plus information on learning opportunities in the field.

Join our networks today!

dbta.com/social-media

database
TRENDS AND APPLICATIONS

cloudera

A Community Approach to Fighting Cyber Threats

Cybersecurity has become the topic of conversation for organizations across every industry as the world continues to become hyperconnected. With the average breach costing $200 per lost customer record, and even more for lost intellectual property, organizations are looking for a new way forward. To make things harder, hackers are a highly collaborative group of individuals that share attack techniques every day. Enterprises, on the other hand, continue to operate individually with very little coordination happening beyond basic threat intelligence sharing. We need to change as an industry.

STOP INDEPENDENTLY SOLVING UNIVERSAL CHALLENGES

As the threat surface expands, the increased number of sophisticated attacks continues to expose organizational vulnerabilities. The tools available to security operations centers (SOCs) are not built for the modern adversary operating in the hyperconnected world. Challenges range from responding to suspicious activity with limited context, discovering advanced threats buried in billions of events, to scaling to the volume of information required to power the SOC.

LONG INVESTIGATION AND RESPONSE TIME

Reducing the mean time to response (MTTR) is a key performance indicator of the efficiency of any SOC and incident response team. Factors pushing the MTTR up can be attributed to the fact that historic data is made unreachable due to archives, necessary data is scattered amongst multiple applications, and important contextual data is not even being collected in the first place.

DETECTING UNKNOWN THREATS

Traditional cybersecurity applications, like security information event management systems (SIEMs), are notorious for their high false positive rates due to their signature and correlation-based techniques (if<A>and<B>then<C>). The detection capabilities are fantastic for known threats, but as the threat landscape gets more complex, hackers are finding ways around these rules. Even if SOCs want to deploy large-scale anomaly detection or behavior analytics via machine learning on enriched data, it's impossible to run these analytics due to the processing limitation of traditional technology.

A NEW WAY FORWARD

While technology advancements have expanded the threat landscape over the years creating massive cyber risk, these advancements have also opened up new cybersecurity capabilities. Cloudera's cybersecurity solution offers unique capabilities through...

UNRIVALED PERFORMANCE, SCALE, AND ANALYTICS

Cloudera's cybersecurity solution is powered by a next-generation data management and analytics platform that breaks down the traditional barriers of data ingestion, storage, processing and analytics. Enterprises can now leverage any type or volume of security data. Cloudera also extends the analytic capabilities beyond simple search and correlation, allowing organizations to deploy advanced statistical and machine learning across larger volumes of enriched data.

OPEN DATA MODELS PROVIDE COMPLETE ENTERPRISE VISIBILITY

Working with the Apache Spot community, Cloudera's solution leverages the community-driven network, user, and endpoint open data models (ODM). This creates a standard schema for critical security data that is siloed across multiple applications. Accessing the open data model provides complete enterprise visibility and enriched data sets for faster investigation and advanced threat detection. Furthermore, storing the security data in the ODM and on Cloudera's open source platform breaks vendor lock-in by disconnecting the data from the application.

APPLICATION FLEXIBILITY

Buy or build applications on top of Cloudera's platform and the ODM to address new use cases while still leveraging the same enriched data set and infrastructure. With multiple Cloudera partners integrating with the ODM, SOCs can now leverage packaged visualizations and machine learning for accelerated detection, investigation, and response. If a vendor application doesn't meet the requirements, enterprises can build custom solutions using open source infrastructure and machine learning algorithms as accelerators without having to incur additional technology costs.

NOW IS THE TIME TO ACT

Cloudera's scalability and machine learning flexibility allow security engineers to build or buy solutions that can run simultaneously on a single, shared, enriched data set and infrastructure. This helps SOCs reduce the mean time to detection and response while all working off of one comprehensive view of the entire enterprise. Using the diverse open source community to accelerate shared innovations, while changing the economics of cybersecurity, allows organizations to come together to fight back against cyber threats.

Get started now at www.cloudera.com/cybersecurity. ■

CLOUDERA
www.cloudera.com

Cyberattack—How to Prepare and What to Do If It Happens

By shifting your mindset from "if" to "when" a cyberattack happens, certain activities which may appear burdensome, tedious, and sometimes are even ignored, will become relevant and important.

By Jacob Cherian

Protecting online systems has become an increasingly difficult job. Over the last decade, we've seen the role of IT security become more critical, not only within the data center, but across entire organizations. The data that a firm has is often its most important asset; hence, it is critical that it is protected. In order to understand how to approach cybersecurity, let's understand what drives the majority of cyberattacks.

Hackers, viruses, and malware have been a part of the internet almost since its conception. The earliest incidents of cyberattacks include the successful hacking in 1983 of computer systems at multiple institutions, including the Lawrence Livermore National Laboratory, and the Morris worm virus infection in 1998 that affected an estimated 6,000 computers and caused an estimated $98 million in damages. Criminals soon realized that illegal access to computers and networks allowed them to steal money, as businesses were increasingly going digital.

The first known ransomware was AIDS, also known as Aids Info Disk or PC Cyborg Trojan, written in 1989. The malware hid files, encrypted file names, and demanded payment to be made in order to receive a fix tool. Since the malware used symmetric encryption, the encryption key could be extracted from the malware data recovery without having to break the encryption. The use of asymmetric encryption for ransomware, first proposed in 1996, changed the landscape of ransomware—data was no longer decryptable by the encryption key in the malware code. The attacker held the key for decryption.

Ransomware turns strong encryption, that was created to protect data, against its users. In addition to this, anonymity in the form of Bitcoin gives the attackers a great way to obtain payment with the certainty that they can't be tracked. Ransomware attacks have become painfully constant; last year, they averaged around 4,000 per day.

Where Is It Going?

Ransomware is an extremely profitable business for criminals. Ransoms paid last year totaled over $1 billion. That's big business. The availability of Bitcoin has created an untraceable form of payment, making it easier for attackers to exploit vulnerabilities remotely, turn encryption into a weapon, and receive ransom. We should also expect to see an increase in attacks, both in frequency and volume. Infosec Institute predicts ransomware to continue rising. Organized crime rings have ventured into this field even without having technical backgrounds. They rely on ransomware-as-a-service servers that hackers have made available in the dark corners of the web.

Even worse, experts predict that ransomware attacks are expected to become more targeted and sophisticated. Ransomware attacks will be launched targeting specific organizations and individuals, and everyday objects such as cars and appliances due to the increasing adoption of IoT.

How to Prepare

The cybersecurity industry has grown tremendously and there are now many ways to protect, prevent, and recover from cyberattacks. It's important to understand holistically that there is nothing that can be 100% secure. The first aspect of preparation is adopting a mindset of "expecting an attack." This allows you to consider your business needs in terms of recovering from an attack and to work backward on determining what you need to do to fill the gaps. It's a matter of thinking "when and how my organization will be a target of a cyberattack," instead of "if."

Every day, new attack vectors and malware scripts are discovered that take advantage of previously unknown vulnerabilities. These so-called zero-day exploits, along with actions that take advantage of known issues (on unpatched systems) and social engineering, pose a formidable challenge for any IT organization. The cybersecurity industry has responded by creating solutions that can deal with known and unknown threats. From software programs that recognize known malware

code, to solutions that can detect unknown threats by identifying behavioral patterns and "virtually" separating them from networks, the solutions for the prevention and detection of malware have grown increasingly sophisticated. Overall, a three-pronged approach is recommended to securing systems and networks from attacks and malware. Let's now look at each of these.

Start With Prevention

By shifting your mindset from "if" to "when" a cyberattack happens, certain activities which may appear burdensome, tedious, and sometimes are even ignored, will become relevant and important. Take, for instance, routine processes such as updates and patching. Although they may seem repetitive and thus sometimes become burdensome, they are still mandatory for any IT organization.

Start with periodic or scheduled port and vulnerability scans and remediate any weaknesses that are found immediately. Network segmentation can limit the exposure to successful attack, and application blocking can prevent malicious code from being able to be run. Improved management of user access by either ramping up password policies or perhaps replacing them with more secure user authentication can prevent unauthorized access. Security experts recommend that it is important that the teams learn from these regular activities by either reflecting individually or discussing as a team how best to introduce practices for specific parts of the environment. By making sure that routine activities have a feedback component, we can convert them into internal projects that deliver valuable learning for the organization.

Educating Users

One of the biggest vulnerabilities in an organization is a human being. Social engineering techniques such as pretexting, phishing and spear phishing, baiting, and others take advantage of cognitive biases that are inherent to human decision making to gain access to systems or introduce malware. Therefore, having a culture of security that makes people aware of these biases and techniques to counter them is critical. User training around security has to be one of the central projects of any IT organization. Hours can be spent designing and implementing a highly secure IT infrastructure, but it can be breached when a single user clicks on the wrong file. Training has to be augmented with clearly defined frameworks and protocols for access to systems and data and periodic testing of those frameworks and protocols.

Detection and Remediation

Quick detection of intrusions or malware in the data center is necesary to minimize the scope and cost of an attack. Detection systems are either signature-based, in which the system looks for known patterns of activity on the network or systems associated with an intrusion or malware, or anomaly based to detect unknown attacks. All anomaly-based systems build a model of what is considered normal and compare current behavior against the model to detect attacks.

Assuming an attack will happen also puts you in the position of having to prepare tools and procedures for remediation. This will save valuable time once an attack has been detected and minimize the impact. With ransomware, this would involve removing the malicious code and decrypting the data. Recovering encrypted data is an option only in the case where researchers have exploited vulnerabilities in the malware code or recovered keys allowing decryption.

Data Recovery

If an attack results in loss of access to critical data, as is the case with malware that corrupts data or ransomware that encrypts your data, data recovery becomes the only option. Recovery from attacks becomes another thing to be considered as you build strategies for data recovery and determine the target RPO (acceptable amount of data loss in case of an incident) and RTO (time to recovery).

Prior to the introduction of snapshots, traditional backups served as the single mechanism for data protection—both for data recovery and for disaster recovery. Traditional backups suffered from very poor levels of RPO and RTO. Snapshots introduced in the early 1990s provided very low RTOs and replaced backup as the preferred mechanism for data recovery from errors and corrupted data, including those caused by malware and ransomware attacks. However, practical RPOs continue to be in the order of hours, with the best achievable at tens of minutes. With increasing frequency of attacks, the sheer volume of data and increased data change rate have meant that using scheduled snapshots still expose customers to significant data loss in the case of a successful attack in addition to the overhead of managing snapshots and schedules. The latest approach to data recovery is "BackDating," an emerging technology that aims to make snapshots obsolete by supporting RPOs as low as 1 second with instant data recovery. This allows for data to be recovered in case of ransomware or malware corruption to the second before the event, and in the case of ransomware, eliminates the need to pay to recover data.

Having a three-pronged approach to security that includes prevention, education, and detection and remediation ensures that you will minimize the risks of not being able to continue operating as a business in case of a successful cyberattack, which is what IT security is about. ■

Jacob Cherian is vice president, product management and product strategy of Reduxio. He is responsible for the company's product vision and strategy, with overall ownership for defining Reduxio's product portfolio and roadmap. Prior to joining Reduxio, Cherian spent 14 years at Dell in the Enterprise Storage Group, where he led product development and architectural initiatives for host storage, NAS, SAN, RAID, and other data center infrastructure.

The Future of Database Encryption

In order for encryption to be more broadly deployed, it must become easier to consume and interfere less with how applications process data.

By Ameesh Divatia

CIOs and CISOs are starting to recognize that database encryption is a critical need and are scrambling to adopt it before their organizations fail the next compliance audit, or worse yet, become a victim of the next major data breach. But there are several hurdles to clear before database encryption is more broadly deployed. Simply put, encryption must become easier to consume and it also needs to interfere less with how applications process data. Enterprise databases have the crown jewels—data that is the lifeblood of how business works—and need to be protected. This is putting the spotlight on database encryption that so far had been a necessary evil that protected enterprise assets when storage disks were stolen.

Today, encryption for sensitive data in databases is available in multiple flavors. There is media-based encryption, where either blocks or files are stored in an encrypted format with the service provider controlling the keys, as well as the encryption/decryption

process; and server-based or transparent data encryption, which is transparent because the applications do not change, and encryption is performed in the database server and the administrator controls the keys. In both of these encryption approaches, the data and the keys are exposed in the server's memory, giving users with access to the database the ability to extract sensitive data with the right tools. To counter this threat, smart application developers use application-layer encryption, where the application performs encryption within its program logic. This usually requires application developers to learn cryptography and key management best practices, identify the right place in the application architecture to perform encryption, and make the right function calls to encrypt and decrypt sensitive data as it is stored in the database. After encryption, the only operation that is possible on encrypted data is an equality check, meaning that nearly all operations previously performed by the application on the data would have to be done after the data is extracted from the database and decrypted in the application. The adjacent table describes each of the approaches and its features. These encryption approaches work, but they are hard to deploy.

PARAMETER	MEDIA-BASED EBS (Block)/S3 (File)	SERVER-BASED (TDE)	CLIENT-BASED (APP-CENTRIC)
Key Management	Controlled at the media level—no customer control	Controlled by database server—could be customer controlled	Controlled by application developer—customer controlled
Encryption Granularity	Entire volume or block	Column or database block level	Column-based
Security Perimeter	Only at the media level. (Any user or process on DB host machine with media access sees data in the clear.)	At the database server level. (Any DB user or application with DB access sees data in the clear.)	At application level. (Only authorized application user can see data in the clear.)
Application Impact	None, other than enabling it during configuration	None, other than enabling TDE using SQL commands	Integrating crypto library and interface to KMS
DB Operations Supported	All. (DB processes see data in the clear.)	All. (Authorized DB users see data in the clear.)	Equality check only on encrypted data in the server

The era of "cloud first" development offers promising alternatives. We are moving to a paradigm of services being programmatically integrated into applications. To follow that model, encryption will be provided as a service so that it can be integrated into existing enterprise workflows with a minimum impact to DevOps practices. This includes centralized orchestration that automates encryption deployment and management and seamless key management that reliably generates, uses, stores, rotates, and retires keys used to encrypt data.

Finally, the service will be delivered on a consumption basis, eliminating the need for hardware-based approaches that have a barrier to entry that restricts encryption to the very high end of the market. The service would be monitored extensively along with the ability to collect audit information that can be used to satisfy compliance requirements stipulated by governments, trade organizations, and privacy groups.

Data encryption is the foundation of an enterprise data protection strategy. For enterprises to reach the critical goal of encrypting all of their sensitive data, they need a new deployment paradigm that makes the process easy to use, provides comprehensive key management, and delivers a true end-to-end monitoring experience. ■

Ameesh Divatia is co-founder and CEO of Baffle, Inc., which provides encryption as a service for databases.

CYBERSECURITY

PROTECTING THE ENTERPRISE

Threats to cybersecurity and data privacy are evolving as infrastructures become less centralized with the rise of cloud, big data, IoT, and mobility. While concerns about risks to data infrastructures continue, research shows that IT organizations are taking steps to mitigate threats with a range of tools and processes.

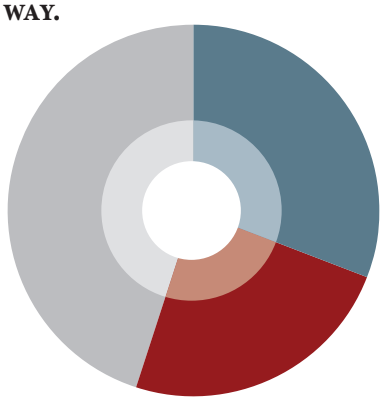
WHILE HUMAN ERROR CONTINUES TO BE A LEADING CAUSE OF DATA SECURITY INCIDENTS, THE COMBINATION OF PHISHING, HACKING, AND MALWARE EXPLOITS HAS BECOME A TOP CAUSE OF INCIDENTS, THOUGH THEY TOO CAN OFTEN BE TRACED BACK TO HUMAN ERROR IN SOME WAY.

In the healthcare, retail, restaurant/hospitality, and financial services fields:

31% of incidents were caused by phishing/hacking/malware

24% were due to employee actions/mistakes

Source: 2016 BakerHostetler Data Security Incident Response Report

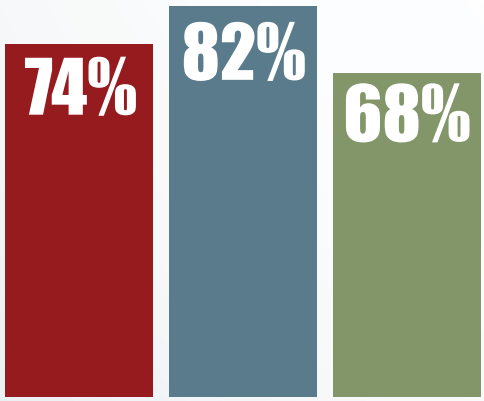


The average consolidated cost of a data breach grew to **$4 million** in 2016, while the average cost for each lost or stolen record containing sensitive and confidential information reached **$158.**

Source: IBM's 2016 Annual Cost of a Data Breach Study Conducted by Ponemon Institute

DIGITAL TRANSFORMATION IS CAUSING IT AND SECURITY LEADERS TO RECONSIDER CYBERSECURITY STRATEGIES AS WELL AS THEIR BUDGET CONSIDERATIONS.

Source: BMC's Second Annual Security Survey, Produced in Association with Forbes Insights (January, 2017)



74% of CIOs and CSOs say security was a higher priority in 2016 than in 2015

82% of executives plan to invest more in security in 2017

68% plan to escalate incident response capabilities in 2017

BY THE NUMBERS

Organizations are becoming more proactive in their embrace of threat intelligence technologies. And, as part of that, cloud-based managed security services are also making inroads in the enterprise.

Tools and processes in place in 2016:

- **52%** have intrusion detection tools
- **51%** actively monitor and analyze information and security intelligence
- **48%** conduct vulnerability assessments
- **47%** conduct threat assessments
- **47%** have SIEM tools
- **45%** use threat intelligences subscription services
- **44%** conduct penetration tests

Source: PwC, CIO, and CSO: The Global State of Information Security Survey 2017

With increased use of cloud technologies comes a range of concerns.

- **70%** of public cloud users believe the tenants using the same cloud resources could jeopardize the security of their own services
- **59%** are equally worried about cloud providers' administrators with privileged access and external hackers
- **48%** believe the public cloud to be inherently more secure than traditional on-premises deployments

Source: "Perspectives from Leading IT Professionals: 2016 IOUG Cloud Security Survey," Produced by Unisphere Research, a Division of Information Today, Inc., and Sponsored by Oracle

Issues relating to data sovereignty have become more pressing in light of new regulations such as the EU's GDPR.

Compliance remains the primary reason for spending on data security **(44%)** followed by concerns about implementing security best practices **(38%)**.

Encryption is the top choice to satisfy data privacy regulations **(64%)** while tokenization comes in second **(40%)**.

Source: 2017 Thales Data Threat Report, Global Edition

Perimeter Protection Is Not Enough

There are three key strategies that organizations should adopt to address cyberthreats and protect their critical data.

By Venkat Subramanian

Across the business sector, the vision for secure business execution is based on the enterprise's ability to safely and responsibly leverage data assets for driving current operations and future strategy. Yet, this is a time of transition in terms of data source diversity, agility in capacity, and access.

More and more organizations are undergoing a major transformation—shifting from IT-led analytics and business intelligence to an approach led by business units with requirements for near-real-time data access spanning on-premises and cloud infrastructure. At the same time, traditional data warehouses are being replaced by new and rapidly evolving big data technology platforms, such as Hadoop and Spark, that are still in their infancy when it comes to data security.

How can companies ensure that their sensitive data stays secure in light of current and ongoing transformations, while also operating within the realm of regulatory compliance?

It's Not Enough to Protect Against Outside Hackers

The common approach to protecting sensitive data is to tighten perimeter security with firewalls, intrusion detection, and intrusion protection. While this is important to thwart external hackers from getting to the data, most of the breaches happen due to bona fide internal users mishandling data. It is this insider threat that needs special attention as more users are provided access.

Volume and file-level encryption touted by platform vendors is good for blanket compliance but not for real protection. A comprehensive approach is needed to cover all aspects of data collection and sharing to protect against external and internal attacks.

Three Key Strategies

To help businesses address cyberthreats and protect their critical data, it is imperative to:

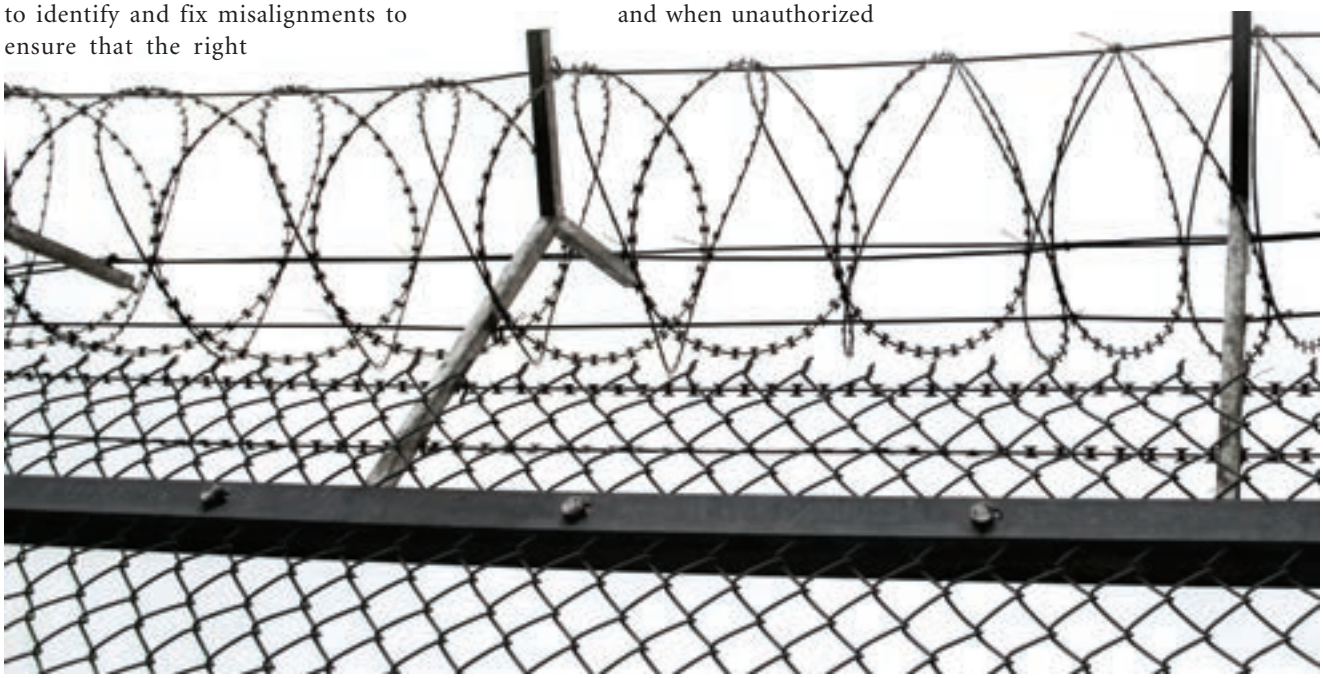
Know your data. The most important requirement is to precisely locate sensitive content in structured, unstructured, and semi-structured data and classify all the files, databases, and other repositories. Next, identify all the groups and individuals within and without the organization who have rights to the classified data in whatever mode they can get to the data. You cannot protect what you don't know.

Protect your data. Sensitivity classification is vital to data protection. First, it is necessary to audit user access to identify and fix misalignments to ensure that the right users have access and lower risk factors. A more comprehensive solution is to provide fine-grained access at the element level. Encryption with access-controlled (RBAC) decryption is the best option, as it helps maximize data access while ensuring regulatory compliance. When "real" data is not necessary, as with summary reporting, masking (one-way obfuscation) is the best protection option. Some masking options allow for the statistical distribution of the data to be retained. Thus, the same summary report would result from the original and the masked versions of data.

Ensure visibility of your data and user access. The natural next step is verification that the process for data classification and protection is being followed and it is working. A single dashboard that manifests data across repositories with associated metadata enables visibility of whether data is classified and protected. Additionally, with a way to turn on alerting on classified data—when accessed, and when unauthorized access is attempted and/or repeated—a more complete picture emerges. Typical tools for monitoring of sensitive data are ineffective with too many alerts that require effort to filter the signal from noise. Combining the use of classification with user definitions of "alertable" conditions makes every alert actionable. The goal should be continuous, near-real-time anomaly behavior detection using machine learning to build a user profile and complex event processing to ferret out potential breaches.

By keeping these pointers in mind, a business has the best chance of ensuring protection of sensitive data and staying compliant with current regulations. ■

Venkat Subramanian is chief technology officer for Dataguise, a data security software vendor based in Fremont, Calif.



How Compliance Affects Data Security

Being audited and verified as compliant can lay a firm foundation for a stable security program, but companies cannot rely simply on security or compliance because they are not the same thing.

By Rob Green

According to the Identity Theft Resource Center, 2016 was a record-setting year for U.S. data breaches, seeing a 40% increase over 2015. With both threats and consumer concern increasing, organizations are placing an even greater emphasis on data security. In this heightened state of security awareness and action, it's easy to assume that organizations are implicitly meeting all the mandated compliance requirements through their security measures. But security does not equal compliance, which has a regimented set of standards that need to be specifically addressed by well-documented, communicated, and implemented policies and practices, according to the specific compliance standard or standards each company is held to. Organizations need a deep understanding of and focus on both security and compliance to best protect data and meet the expectations of consumers, the organization's board of directors, stakeholders, and compliance governing agencies.

Understanding Compliance

The two most dominant and far-reaching compliance standards are:

- PCI Compliance—Protecting payment card data
- HIPAA HITECH Compliance—Protecting personal health information (PHI)

Both measures were put in place to protect sensitive data from being mishandled and exposed, particularly as personal financial and health information continue to become more valuable on the black market.

Both PCI and HIPAA HITECH compliance require organizations to follow set standards in order to attain compliance and perform regular audits to maintain good standing. As these standards are specific and can be confusing, it's best to work with a compliance professional or solution providers that can provide elements of compliance. Relying on the chief security officer or chief information security officer can mean organizations miss the finer details of compliance. CSOs and CISOs are concerned with a broader array of issues and aren't specifically compliance experts.

It's important to remember that, in many cases, organizations that aren't the point of collection or origin for sensitive data must also meet compliance standards or a variation thereof. Don't dismiss compliance simply because you think it "doesn't apply to you" or because you rely on security measures that are totally detached from compliance requirements. Any data management vendor or service provider that stores, transmits, or otherwise provides access to a customer's data, which may include PHI and/or credit card information, will likely be held to some level of compliance requirements. A breach at the service provider or vendor level can expose data just as easily as a breach at the data's point of origin.

Common Myths About Compliance and Data Security

There are many misconceptions about compliance and data security. The ever-evolving nature of compliance standards and the fast-moving threat landscape have organizations scrambling to understand who needs to be compliant, what that takes, and how far compliance reaches.

These common myths and misconceptions can lead organizations into dangerous, unprotected territory.

MYTH: If I have a compliant service/solution in place, I meet compliance requirements.

Whether you need to meet PCI compliance, HIPAA HITECH compliance, or another compliance standard, the requirements are specific and far-reaching. As such, no single service or solution will satisfy all your compliance requirements or negate the need to complete regular audits.

For instance, simply operating with a verified compliant desktop solution—or any other singular element—doesn't mean your data is compliant or protected at any other stage of access, transmission, or storage. When implementing any services or solutions, it's a good idea to involve a member of your compliance team, and even a third-party auditor, to understand what requirements that solution solves, how it can help with future audits, and if it meets the organization's needs (or is a redundant compliance effort).

MYTH: If I'm HIPAA-compliant I'm also PCI-compliant, and vice versa.

HIPAA HITECH and PCI compliance standards are completely independent from one another with separate governing bodies and their own unique set of requirements. While obtaining a service/solution that meets one set of requirements may help you more easily meet another compliance standard, it's important that the solutions you put in place are independently audited and verified for every compliance standard your organization abides by.

In the future you will also have to complete all the necessary audit and reporting requirements for each standard that applies to your organization.

MYTH: I'm not a healthcare provider so I don't need to be HIPAA-compliant.

HIPAA HITECH compliance is designed to protect personal health information (PHI) anywhere it goes. Therefore, any company that collects, transmits, accesses, stores, or otherwise handles PHI may be covered by all or a portion of the HIPAA HITECH compliance rules.

The standard specifically pertains to:

Covered Entities

- Healthcare providers
- Health plans
- Healthcare clearing houses

Business Associates

- "A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity," such as claims processors, translation and transcription services, CPA/legal services, consultants, benefits managers, etc.

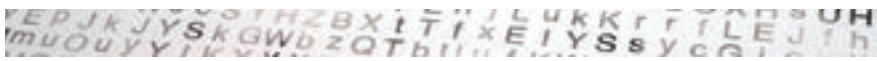
In many cases, companies that are not specifically within the healthcare vertical but who service the healthcare industry and work with PHI will be asked to sign a Business Associate Agreement (BAA) and meet HIPAA HITECH compliance standards. This is particularly important for data management vendors and solution providers—such as a desktop-as-a-service provider—as these organizations could handle PHI when servicing customers and thus be held to HIPAA HITECH compliance standards.

MYTH: We have security policies and procedures in place, so we're compliant.

While both compliance and security are important for covered organizations, it's not enough to rely on one team or one implementation plan to cover all the necessary facets of both security and compliance. For instance, even if data is encrypted, it may not meet all compliance standards for full protection, which also includes:

- Physical data center requirements
- Roles and responsibilities
- Encryption strength
- Data destruction policies
- Offsite back requirements
- And more

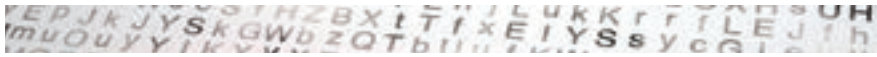
On the flip side, while compliance accounts for many risk factors, companies may find that their data is best protected when additional security measures that are not mandated by compliance requirements are also put in place. It's important not to confuse security with compliance, or compliance with full-fledged security.



*Organizations need a deep understanding of and focus on both **security and compliance** to best protect data and meet the expectations of consumers, the organization's board of directors, stakeholders, and compliance governing agencies.*

Compliance Does Not Equal Security

That last myth leads to a very important point: Security does not equal compliance and vice versa. Having a strong security posture often helps organizations meet compliance requirements more easily, and being audited and verified compliant can lay a firm foundation for a stable security program, but companies cannot rely on simply security or compliance because they are not the same thing. For instance, the famous Target data breach of 2013 occurred only months after the retailer was deemed PCI-compliant, proving that while the organization met the specific requirements for compliance, its data was not truly or fully secure.



The ever-evolving nature of compliance standards and the fast-moving threat landscape have organizations scrambling to understand who needs to be compliant, what that takes, and how far compliance reaches.

Compliance

The hallmark of any compliance standard is that it is tied to a detailed, documented set of specific requirements organizations must meet in order to be deemed compliant. This detailed set of requirements is one of the reasons compliance does not equal security. While the standards are in place to create a tight security net, its reach is inherently limited by the very fact that it is a documented—and potentially outdated—list of requirements. This means any risk or security concern not covered by compliance requirements could create a security hole.

It's true that almost all of the individual compliance requirements tie directly to security-related measures, and a thorough compliance program can be an important part of a strong security program. However, compliance essentially boils down to a (very important) reporting function or form of demonstrable security—"proof" that you have specific security measures in place. Because of this, compliance is finite, something you can "complete" (albeit on a rolling basis), unlike its wider-reaching cousin, security.

Security

Security is more abstract and undefined than compliance, meaning it can have a farther and more impactful reach. One of the best ways to demonstrate the difference between compliance and security is to think about how quickly the security threat landscape changes compared to how quickly any regulation can be updated, reviewed, rolled out, and implemented. While compliance standards are regularly updated, the sheer fact that they are regulated sets of requirements means they will never move fast enough to keep up with the quicksand environment that is cybersecurity and data risk.

Unlike completing a checklist of requirements, the impetus for security decisions is sheer demand. A new threat arises, and new policies, procedures, and protections are put into place to address that threat. Security affords organizations more flexibility in how they address certain risks, allowing for innovation that could lead to a stronger security environment.

Essentially, you can't have compliance without security, but compliance itself is not enough to protect an organization. Teams need to constantly identify gaps not covered by compliance requirements or new concerns driven by new threats. Compliance is a piece of security, but it's not large enough alone.

Better Together

In the end, we can all agree that when it comes to data security, the more protection, the better. While compliance standards don't offer total protection, they do create a solid and consistent set of standards for organizations to follow, creating a baseline for data protection.

The organizations that are most successful at preventing breaches appreciate the importance but also the place of compliance. They also understand that compliance alone is not a stand-in for security. The two need to work together to collectively create a complete environment.

For organizations struggling to get a handle on data security, pursuing compliance verification is a good starting point to lay a security foundation. From there, the organization can address and fill further security gaps. For organizations with mature security programs, becoming compliance verified can further shore up protections and possibly identify some weaknesses.

Both security and compliance require specific attention and active measures, but together they can form stronger protection for your company, your customers, and your data. ■

Rob Green, CTO of Dizzion, oversees all aspects of technology, including strategy, infrastructure, systems, tools, and development. Before Dizzion, he was the executive vice president of cloud services at MDSV, a leader in hardware, services, and integration, responsible for defining product and marketing strategy for the MDSV open integrated hardware server platform.

Security and IoT

To ensure IoT data protection, the combination of infrastructure, people, process, and technology must be a top priority.

By John M. Hawkins

The Internet of Things (IoT) continues to gain momentum. The number of connected IoT devices—from refrigerators to health devices—has been projected to grow at an annual compound rate of 23.1% from 2014 to 2020, reaching 50.1 billion things in 2020, according to recent research. Whether or not the number of devices linked to the internet reaches this lofty number in the next 3 years, it is clear that the growth in sensors and gadgets is explosive. The question is: If devices continue to advance rapidly, then how will all of this data stay protected, private, and secure?

The consumers' appetite for easy, always-on, and everywhere access seems to be insatiable. For instance, when a shopper forgets his or her grocery list at home, there is now the ability to virtually check inside their refrigerator to see if they need eggs or milk. This type of IoT device capability is growing faster than expected, which adds pressure on the infrastructure, people, process, and technology that keeps everything functional. The catch is that these new uses of IoT devices are opening up endpoints on networks, which translate to potential security issues—and in some cases, these devices are broadcasting information, providing a prime target for cybercriminals to look for vulnerabilities.

To keep these platforms secure, the brunt of the responsibility will rest on the shoulders of the producers of these "things"—keeping the dynamic data and information that is surging throughout the IoT platforms protected and safe, as well as the physical and virtual infrastructures that house it all. While many are thinking about the associated security risks, most are not aware that technology only solves a portion of this. To ensure IoT data protection, the infrastructure, people, and the process are also important.

There are many risks to consider as pertaining to IoT. In fact, TechRepublic recently reported that more than 90 million cyberattacks are estimated to be registered in 2016, which means 400 hacks every minute. As data travels through a virtual ecosystem, security must extend beyond the device itself. This means that having information and physical security in place, along with the right people and process to monitor and proactively test security, are all critical to maintaining a secure environment. Therefore, there must be layers of protection and controls in place at all levels to separate the "strongest" secure data center from the weaker, or more vulnerable, facilities and systems.

Technology Safeguards for IoT

Network Routes to IoT Management Systems and Devices: The route to the IoT management interface, as well as the devices

themselves, could open up additional security vulnerabilities. IoT devices by definition communicate; they either push data upstream to a managed system or may be polled for data. The API's open ports are all opportunities for malicious hackers to see what protocols are running and potentially expose a weakness.

Social Engineering of Those Who Manage IoT Platforms: In certain cases, the attack can be the result of an innocent-looking request that was sent to a system administrator—who accidently clicked on it—thereby giving access to the hacker to get into the system.

Updating IoT Device Firmware: It might sound simple, but checking and updating the firmware can keep you one step ahead of those wanting to exploit the IoT devices. If there is an IoT device exploit, the manufacturer will typically identify and fix the issue before a hacker has the ability to gain access to your device's environment.

Default Passwords: One area that most don't think of is the default password. Devices typically will come with a default password that most think are "non-threatening"—meaning those that don't hold sensitive, detailed information—such as a home's smart thermostat. However, that may not be the case, given that these devices might have a way to communicate back to the IoT management platform.

Back to Basics: The concept of putting a device on a network isn't necessarily a new idea—developers have been solving this design challenge for years. Recall that software architectures have evolved and changed. For example, think about the many various software architectures we have seen over the last 25 years such as standalone, fat clients, client server, thin clients, and now device-to-server. By going back to the basic security tenets we use for other platforms, this also applies to the IoT platforms.

Ask Questions of Your IoT Vendor: In many cases, this means that we need to ask all the questions that we asked with the prior platform architectures and also "test" for vulnerabilities. These include: How does the device capture, store, and transmit data? Is the device data encrypted? Is the data on the device pushed or pulled to the IoT management interfaces?

Infrastructure + People + Process

The physical security features of a data center facility, such as doors, cameras, and sign-in sheets, are critical, but these measures alone can be compromised. This is why there must be properly trained staff and controls in place to maintain a secure data center that will support all of these platforms. All data center employees must conduct annual security awareness training—so that they can be up-to-date with the latest threats and potential issues.

Training of people must go beyond just those who manage the data center. It's important to make everyone—from operations, IT, even sales and marketing—who has access to the data center aware of these security risks and what it means to them. Any employee who lets in a tailgater can compromise the infrastructure, people, and process. It's pivotal to train staff on the IoT platforms so that they get an appreciation for the technology aspect—having a solid understanding will give a better idea with regards to what they should be looking for.

These lingering threats require active measures. You'll see information security standards such as ISO 27001 becoming more prevalent to ensure that there is more in place than just tools. This certification is an excellent example of engaging the whole company in security and compliance initiatives and ensuring that additional controls are in place to help test the overall effectiveness of their information security management system (ISMS).

Infrastructure, people, process, and technology are key areas of focus that can bolster the security within the data centers that hold the IoT data. But let us not forget about some of the other risk factors when it comes to IoT.

IoT is changing the way we think about devices and applications. It's forcing more and more devices to interface with one another on a common network (i.e., the internet). Putting a device on a network certainly isn't a novel concept—and in many cases, having preventative measures in place can help if there is a massive infusion of devices on a common network that may open the door to a whole new set of opportunities for hackers and exposures never before contemplated. Many of these devices are built and managed by companies and people who put functionality as the top priority as opposed to security.

What's Ahead

Companies need to take a proactive approach to IoT security to determine that they have the proper controls and policies in place. Policies are there to protect the business, to help make sure everything is in order and "working as normal" so that clients within the data center can rest assured that the infrastructure, people, process, and technology are in place to support the platforms. Security procedures, such as incident response, disaster recovery, and business continuity plans, should be a top priority for businesses dealing with the heavy loads of IoT data.

While these new devices are designed to make our lives easier, there is always the threat that social engineering or not asking the right questions can lead to IoT device vulnerabilities that could be used as a launch pad for doing harm. These are just a few thoughts that need to be considered when it comes to IoT security risks. ■

John M. Hawkins, vice president at vXchnge, is an author, speaker, writer, strategist, and technologist, with more than 20 years in business as a consultant to Fortune 25-500+ companies. Previously, Hawkins was a senior director for RiverMeadow, a Silicon Valley-based SaaS company, where he was instrumental in helping to define cloud mobility and providing services to large cloud providers.

Deploying Robotics for Data Center Security

A robotic technology that can connect or disconnect a network connection physically and quickly introduces more security and manageability.

By David Wang

IT MANAGERS UNDERSTAND that it is best to be proactive rather than reactive. Setting up proactive measures and thinking ahead about how to handle security issues will set up a data center for success.

The amount and complexity of attacks from both outside and inside sources continue to grow, making IT security and risk mitigation full-time tasks. Currently, security concerns are addressed by deployment of purpose-built applications for the detection, monitoring, and quarantining of common known attacks from outside sources, as well as firewalls for both solidified perimeters and internal segmentation.

Additionally, inside threats have been tackled by multiple software-based policies, siloed departments and access control, password or authentication technologies, and other advances such as auto-redaction. Is this all there is though? Are there other areas that can be advanced to quell concerns when it comes to security?

An area that present security approaches don't address is the infrastructure itself. With the static nature of the network infrastructure in the data center currently, IT must take a very hands-on approach to making and maintaining connections so that business can move forward. This not only leads to more money and time being spent to manage growing data centers, but also introduces potential security threats to them and impacts a business' ability to react in the event of either malicious or unintentional breaches.

Today's data centers are sprawling millions of square feet, and efforts to secure them continues to grow. IT managers must consider ways to make infrastructure more dynamic so it will be easier to respond to and control points of vulnerability. From our experience, we suggest that IT managers look to robotic automation. Robotics presents a very compelling case and can be leveraged to significantly improve data center security response. Two key security areas of concern that robotics can save your data center from are risk of human error and response lag time to a threat.

Risk of Human Error

In the words of Alexander Pope, "to err is human." We're all human, we make mistakes. Whether a malicious attack or simple mistake, human error can pose a serious risk to a business and its data. The security threats posed by traditional viruses, Trojan horses, and other common methods are well-known and documented and currently protected against by advanced firewall and other appliances. While this is important, what many seem to forget to consider and address is another important point of vulnerability—the infrastructure itself.

All optical connections within a data center, as of present, are monitored and managed manually. Why is this a key security issue? Because of the risk of miscommunication or other human error. This risk increases the potential for a wrong move to be made when performing simple maintenance or making adjustments to network infrastructure, leading security threats to quickly become bigger problems. This can also lead to an unplanned outage and downtime.

To combat this, many have implemented a redundancy plan or created a data center resiliency strategy, usually associated with other disaster planning and disaster-recovery considerations. While this approach can be helpful when running into issues due to human error, it doesn't actually solve the issue itself—preventing human error. Furthermore, it typically leads to an increase in upfront purchase costs and can escalate energy bills. To concretely prevent security threats from happening, the potential for human error needs to be addressed directly. Finding a way to automate manual connections and removing the possibility for human error will simplify monitoring of potential areas of exposure and, in the process, will help save money and time.

Response Time to a Threat

The difference between a simple fix and a big nuisance is the time it takes to react to a security threat. Specific things need to be done very quickly to cut off the bridge and to reroute the traffic in order to evade the possibility of the threat spreading further. Physical connections in remote data centers today have to be changed manually, meaning a company is only as fast to respond as it can dispatch an operator and get to work on solving the threat.

The amount of time it takes for people to travel, to get on the phones, and to get to the data center to fix the issue is a serious factor in data center security, as it can take anywhere from days to weeks to respond, especially when working with remote micro-data centers. Another contributing factor to the amount of time it takes to respond is the static nature of the infrastructure. The valuable time that is lost in all of this gives security vulnerabilities longer to propagate, potentially exposing additional machines and servers. In the data center, time is always of the essence, especially when it comes to dealing with a threat.

Additionally, with the high volume of security alerts received and needed to differentiate from real threat and false positive, it is even more vital that response time is as fast as possible. By taking a more proactive approach to the infrastructure and enabling it for dynamic, remote management, businesses can substantially improve time-to-response and enable IT to quickly mitigate any risk.

Robotic Automation to the Rescue

While robotic automation has been around for quite some time, it is still in its infant stage. Some feel that robots will replace jobs and complex business practices, but that is not the case. Robotics allows for IT staff to focus on more high-level business and projects, increasing productivity and creating a more automated environment. The IT staff is also a vital part in making robotic automation work, as it is just an extension of the staff, since they have to direct and tell the technology what to do. It essentially improves the job of IT professionals because it enables them to have full control of physical fiber connections, allowing changes to be made automatically, remotely, quickly, and without manual intervention, thereby diminishing the threat that human error and long response time can pose to data center security.

When it comes to setting up and building a more robust and simple network, a robotic technology that can connect or disconnect a network physically and quickly introduces more security and manageability, as well as peace of mind. Network operators will not only see security response improve as a result of the introduction of robotic technology for managing the physical optical connections within, they will also see reduced OPEX and CAPEX, improved reliability, which will make their critical infrastructure future-proof.

With robotic automation in the data center, security concerns can be reduced dramatically. Placing traditionally manual tasks into the "hands" of robots makes data center networks more secure and makes it possible for security issues to be resolved in real time from anywhere, with no concern for potential human error or lag time. Robotics in the data center contributes to making IT infrastructure more agile and less expensive and can help decrease the overall data center footprint as well as infrastructure complexity.

Incorporation of robotic automation also allows for the data center network infrastructure to be simplified and more dynamic and can aid IT staff in quarantining threats by quickly eliminating connections to other systems remotely. IT managers can send a software command to the robots in the data center and, with the click of a button, manage hundreds of fiber connections. Currently, connectivity is run in the data center with various different layers of technology and protocols, making the network complex and leaving it open to vulnerabilities. Introducing robotic physical optical connectivity, and the ability to set up a physical connection through software with application control (often called SDN), alleviates this. The software of the application can try the connectivity when needed, as needed.

In the future, hopefully within this year, we will see the advantages of robotic automation on data center security advancing even further with the layering of AI. When deployed alongside the robotic technologies, AI will allow switching of connections within the network based on network setting and real-time traffic, freeing up time from monitoring and directing these adjustments. This will increase the removal of potential human error and improve response time, creating an even more secure data center. However, the layering of AI on robotic automation in the data center is a story for another time.

IT managers understand the significance of keeping the data center secure and, as such, should strongly consider integrating robotic automation. ■

David Wang is CEO of Wave2Wave Solution, a data center connectivity company headquartered in California.

Data Protection as a Key Enabler of Digital Transformation

Establishing and maintaining consumer trust must be every organization's goal in the evolving digital world.

By Miller Newton

Though the world has been online for more than 20 years, we are only beginning to see how digital technology will change the way we work and live. Online transactions, paperless communication, and mobile apps were just the first steps in an evolution that is not only making business faster and more efficient, but is changing our ideas about what is possible.

We have entered the era of digital transformation, where businesses—and consumers—are continually rethinking their goals and priorities in light of emerging technologies. Restaurants use mobile apps to take reservations and orders. Running shoes track their owners' speed and distance. Even farm crops and livestock can be managed electronically. In this environment, every company is a technology company.

While the trend is almost universal, each organization's digital transformation is unique. Some companies reinvent their internal business processes, some find new ways to interact with their customers, some develop new products and services, and some do all of the above. The phenomenon is by no means limited to brick-and-mortar businesses that are building their online identities. Even internet startups are learning that they must transform their own business models to stay relevant as technologies and user behaviors evolve.

Ever-Expanding Data

However an organization transforms, it is certain to find itself generating, collecting, and using more data with each step it takes. New devices, new workflows, and new forms of customer interaction all contribute to the ever-increasing volumes of information that organizations must manage in the digital world. A recent Cisco report estimated that global data transfer volume would exceed 1 zettabyte (one trillion gigabytes) for the first time in 2016, and would double again in just 3 years.

Enterprise data is increasing not only in volume, but in importance. Every single bit of that zettabyte of data has value to the organizations that create, transmit, or store it. Companies are making decisions more quickly than ever before, and in order to do so, they require accurate, up-to-date information from a variety of internal and external sources. Even a small amount of compromised or unavailable information can set an organization on the path to missed opportunities and lost profits.

Most significant of all is the increasing sensitivity of the data that organizations are collecting and processing. Personal details, financial records, healthcare information, and other forms of sensitive data are passed between consumers, corporations, and government agencies on a continuous basis. The expanding Internet of Things (IoT) has created a new realm of high-value information, with the potential for unprecedented damage in the event that something goes wrong. As we move more of our lives into the digital universe, we become exponentially more vulnerable to digital threats.

The New Importance of Security

Given the increasing volume, importance, and sensitivity of business data, it is no surprise that information security has taken on even greater importance in the era of digital transformations.

Larger, more valuable datasets are naturally more appealing targets for data thieves and other hackers. No one needs to be reminded of the high-profile breaches that have exposed the secrets of corporations and government entities around the world in recent years. It is worth noting, perhaps, that data breaches now have the potential to affect hundreds of millions or even billions of people, as evidenced by the latest revelations from Yahoo. A single security weakness can have truly worldwide consequences.

In addition to potentially devastating lawsuits from affected users, organizations now face the prospect of heavier regulatory penalties when they lose consumer data. The new General Data Protection Regulation (GDPR) in the EU, for example, will allow for fines up to 4% of annual revenue for companies that fail to protect the sensitive data of European citizens. Other jurisdictions are likely to enact similar laws as concerns about personal data continue to grow.

The most important purpose of information security, though, is not to avoid punishment, but to build and maintain consumer trust. Even the harshest financial penalties are just a fraction of the long-term cost that a security breach can inflict.

Today's consumers expect their information will be kept safe by every organization with which it is entrusted, and failing to do so can leave a company permanently behind in the race to build and enhance its enterprise. Not only will customers hesitate to trust a company after a breach, but other businesses will be reluctant to enter into partnerships with it, for fear of damaging their own reputations.

Companies can suffer from inadequate security even in the absence of a data breach. It is not enough to simply stay out of the headlines—businesses today must actively demonstrate that they have taken steps to secure their sensitive data. As consumers become more aware of cyberthreats and more savvy in their decision making, organizations who fail to commit to data protection will watch their customer lists dwindle. Companies that compete for government contracts or do business in regulated industries will find themselves on the outside unless they keep up with the latest security standards.

What we have seen is that forward-thinking organizations now view security as something that can enable new growth, rather than an obstacle to business as usual. In order to create new experiences for customers, every company must be able to collect, process, and share information across computing platforms and among multiple partners. The only way to do this—and to maintain customer trust in the long term—is to build data security into the very foundation of everything an organization does. It's no exaggeration to say that information security is one of the fundamental requirements for successfully completing a digital transformation.

Protecting Data, Not Networks

Not only do organizations need to give information security a new place in their business models, they need to change the focus of their security activities. Data protection, rather than network or device protection, is becoming the top priority in the new digital environment.

Focusing on data protection means taking a fundamentally different view of the goals of information security and of the tactics and strategies needed to achieve those goals. Rather than investing in additional layers of hardware and software intended to keep intruders out, organizations that adopt a data-centric security strategy have shifted their attention to what thieves and spies are actually interested in: the sensitive information stored on an organization's devices and networks.

Preparing for the Inevitable

The data-centric approach to security acknowledges the simple fact that no wall is ever high enough. If a company has something worth stealing, eventually someone will manage to steal it. Network and device protection cannot withstand today's highly sophisticated, often state-sponsored, cyberattacks, and these traditional strategies are even less relevant now that cloud services and mobile devices are central elements of enterprise architecture. After all, how can a company secure its network from internet threats, when its network is the internet itself?

Assuming that your data will be stolen, however, is not the same as assuming it will be compromised. Data-centric protection renders information inaccessible to anyone but authorized users. When data itself is protected, it becomes useless even when lost, stolen, or mishandled.

Strong encryption is the most reliable form of data protection and is rapidly gaining popularity, despite efforts by lawmakers in various countries to compromise it. Widely used encryption algorithms such as AES-256 provide exceptional security against even the most well-equipped hackers. In fact, even if a data thief had access to every computing resource on the planet, it would take billions of years to break an AES-256 encrypted file using a brute-force attack.

The Age of Encryption Has Begun

Data encryption, realistically, is the only hope for organizations that want to keep their sensitive data safe. Many industry groups and government agencies now demand that companies use strong encryption to protect sensitive data, and these requirements will only become more prevalent in coming years.

Encryption can also insulate an organization against regulatory actions. The European Union's GDPR recommends the use of encryption and specifically exempts companies from punishment if they suffer a security breach but had applied strong encryption to the data before it was stolen. Again, though, compliance with industry or government mandates is only a secondary reason to move toward data-centric security. Establishing and maintaining consumer trust must be every organization's goal in the evolving digital world, and safe data is the foundation on which that trust must be built.

In the years ahead, as data volumes grow to unimaginable sizes and cyberthreats grow even more sophisticated, the companies that build data protection into their identities will be the ones that shape our future. ■

Miller Newton, president and CEO of PKWARE, joined PKWARE in 2009, after serving as CEO of Netkey, which was acquired by NCR. Prior to Netkey, Miller was chairman and CEO for Boston-based Lavastorm Technologies (now Martin Dawes Analytics), CEO of Monster, and executive vice president of sales and marketing for TMP Worldwide, a global marketing and communications company and parent company of Monster (now Monster Worldwide).

BDQ

BIG DATA QUARTERLY

THE NEW PUBLICATION FOR THE ERA OF

BIG DATA

Brought to you by the editors of *Database Trends and Applications* magazine, *Big Data Quarterly* is for information management and business professionals who are looking to leverage big data in organizations of all kinds. Subscribe today and stay informed on big data, data science, and the technologies and business strategies surrounding them.

This is a must-read publication for data scientists, CIOs, and other professionals involved with big data projects.

LIMITED-TIME FREE OFFER!* SUBSCRIBE NOW.

dbta.com/BDQ/Subscribe

*Free to qualified U.S. subscribers.
Regular subscription rate is $95 per year.

Since 1978, IRI, The CoSort Company, has continued to deliver robust data movement and manipulation software for IT managers and developers whose data grow faster than their budgets. In 2007, for example, IRI was the first company to mask fields in files (off the mainframe).

Similar IRI innovations and price-performance advantages are available today for data-centric security professionals who need:

- PII discovery and classification
- Easy, multi-source data masking
- Safe, referentially correct test data
- Fast, no-impact DB firewall technology

These tools are now also bundled in the award-winning IRI Data Protector suite.

Learn more at:

www.iri.com/products/iri-data-protector

+1.321.777.8889
info@iri.com

PROVEN, AFFORDABLE DATA-CENTRIC SECURITY
www.iri.com

MENTIS: The most advanced application & data security platform. Unparalleled discovery supports static and dynamic data masking, continuous monitoring, and retirement solutions for security and compliance. MENTIS' masking brings the ONLY conditional and location-aware DDM capabilities available; tokenization and format-preserving encryption anonymization methods include customizable libraries.

MENTIS' products are designed to share sensitive data intelligence and a common database architecture. Benefits include clear SOD capabilities and ease-of-implementation through low-overhead/high-performance architecture. The platform enables customers to secure at-risk data across its lifecycle, in on-premise, hosted, and cloud environments, and on Production, Pre-Production, Non-Production, mainframe and relational databases; and file servers.

MENTIS Software
3 Columbus Circle • 15th Floor
New York, NY 10019 • 800 267 0858

Contact:
Harriet Schneider • Vice President, Marketing
harriets@MENTISoftware.com

MENTIS SOFTWARE
www.mentissoftware.com

Cloudera empowers cybersecurity innovators to proactively secure the enterprise by accelerating threat detection, investigation, and response through machine learning and complete enterprise visibility. Cloudera's cybersecurity solution, based on Apache Spot, enables anomaly detection, behavior analytics, and comprehensive access across all enterprise data using an open, scalable platform.

CLOUDERA
https://www.cloudera.com/solutions/cybersecurity.html

Oracle helps secure and manage heterogeneous hybrid cloud environments by providing an intelligent platform which can detect, prevent and respond to security and management risks with minimal additional burden on already-overwhelmed staff. Cloud-scale analysis based on machine learning provides smarter, real-time insights into potential and active security and performance issues, and automated remediation ensures swift action. Designed for the scale and complexity of digital business, hybrid cloud and big data, Oracle offers customers a next-generation solution to secure and manage both new hybrid cloud and traditional environments.

Contact info: 1-800-633-0738 (US)

ORACLE
www.oracle.com/security

Cloud **Essentials**

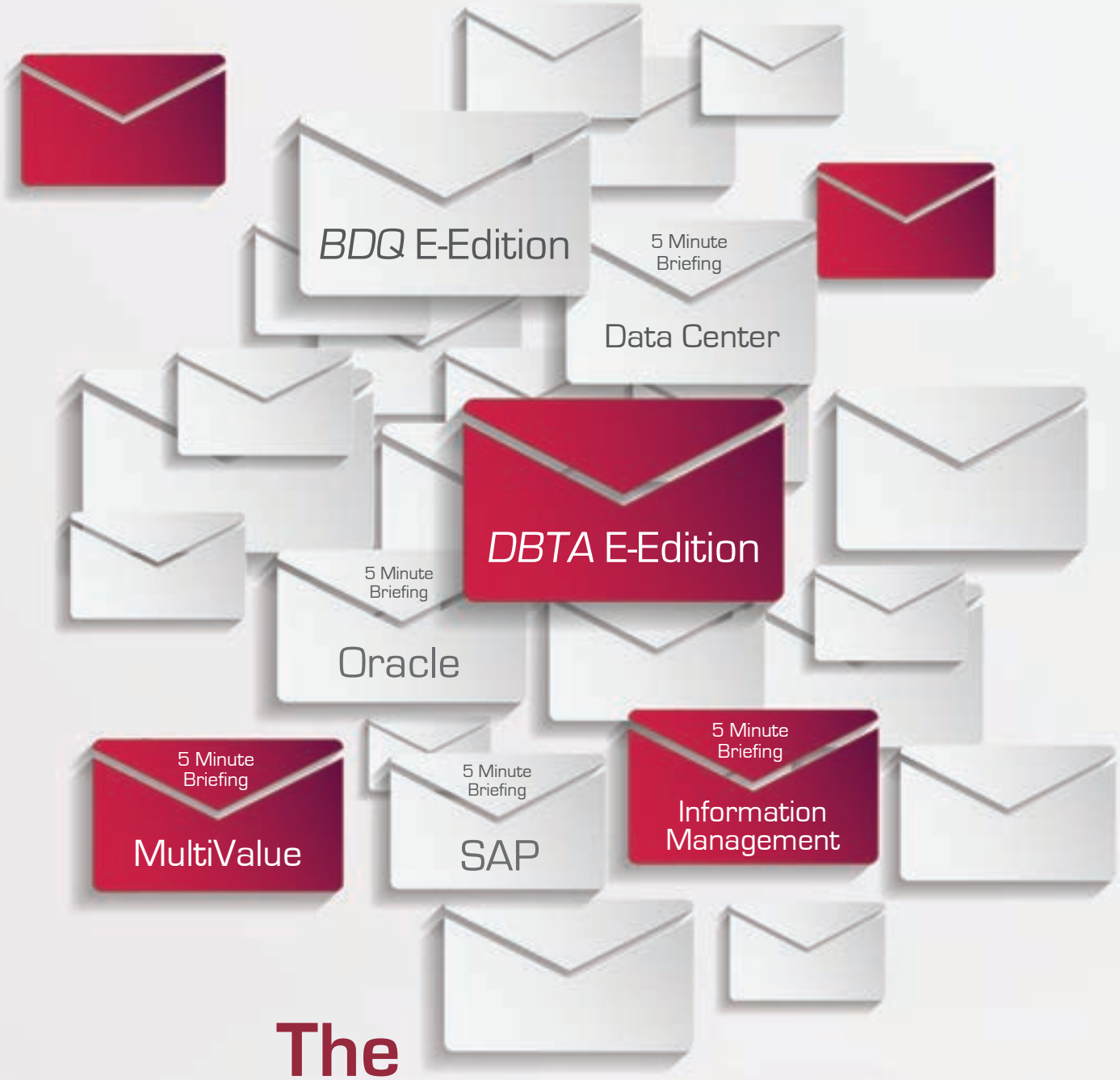
Oracle Cloud Platform

- ☑ **Complete**
  Best-of-breed and integrated solutions in every cloud category of data, software, platform, and infrastructure
- ☑ **Open**
  Standard-based platform that supports all workloads, apps, languages, open source, and data types
- ☑ **Secure**
  Automatic, always-on protection pushed down the entire cloud stack to the silicon layer
- ☑ **Choice**
  Flexible deployment options in public, private, Oracle Cloud at Customer, and hybrid cloud
- ☑ **Intelligent**
  Artificial intelligence and machine learning in every cloud category of data, software, platform, and infrastructure

Request a security assessment from your local sales team, and visit oracle.com/security to learn more.

Connect with us

ORACLE



The MOST INFORMATIVE mail in your inbox.

Database Trends and Applications produces seven original email newsletters, each with targeted content on specific industry topics. Receive concise reports on what's happening in the data world—straight to your inbox! Now offering *5 Minute Briefing* newsletters, *DBTA* E-Edition, and *Big Data Quarterly* E-Edition.

database TRENDS AND APPLICATIONS

BDQ BIG DATA QUARTERLY

Subscribe today!

dbta.com/newsletters