Volume One / Issue Three

BANK OF AMERICA

Cyber Security Journal

The latest ideas on digital security to help you safeguard what's most important to you

WAYS TO PROTECT YOUR MOST VALUABLE DATA

Enterprises create more data every year: How can governance keep up with the volume?

KEEPING NETWORKS ACCESSIBLE AND SECURE

How companies can leverage the right tools and privileges to protect their critical systems.

HOW TO REDUCE THIRD-PARTY CYBER SECURITY RISK

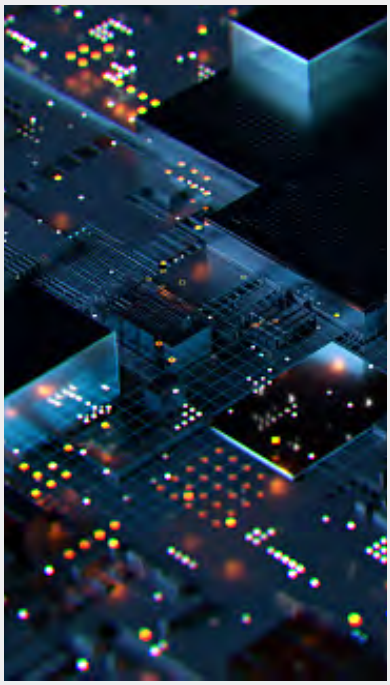
Outsiders have more access to the enterprise than ever before, but are they as secure as you are?

Contents

Cyber Security Journal • Vol. One / Issue Three

Letter

Features



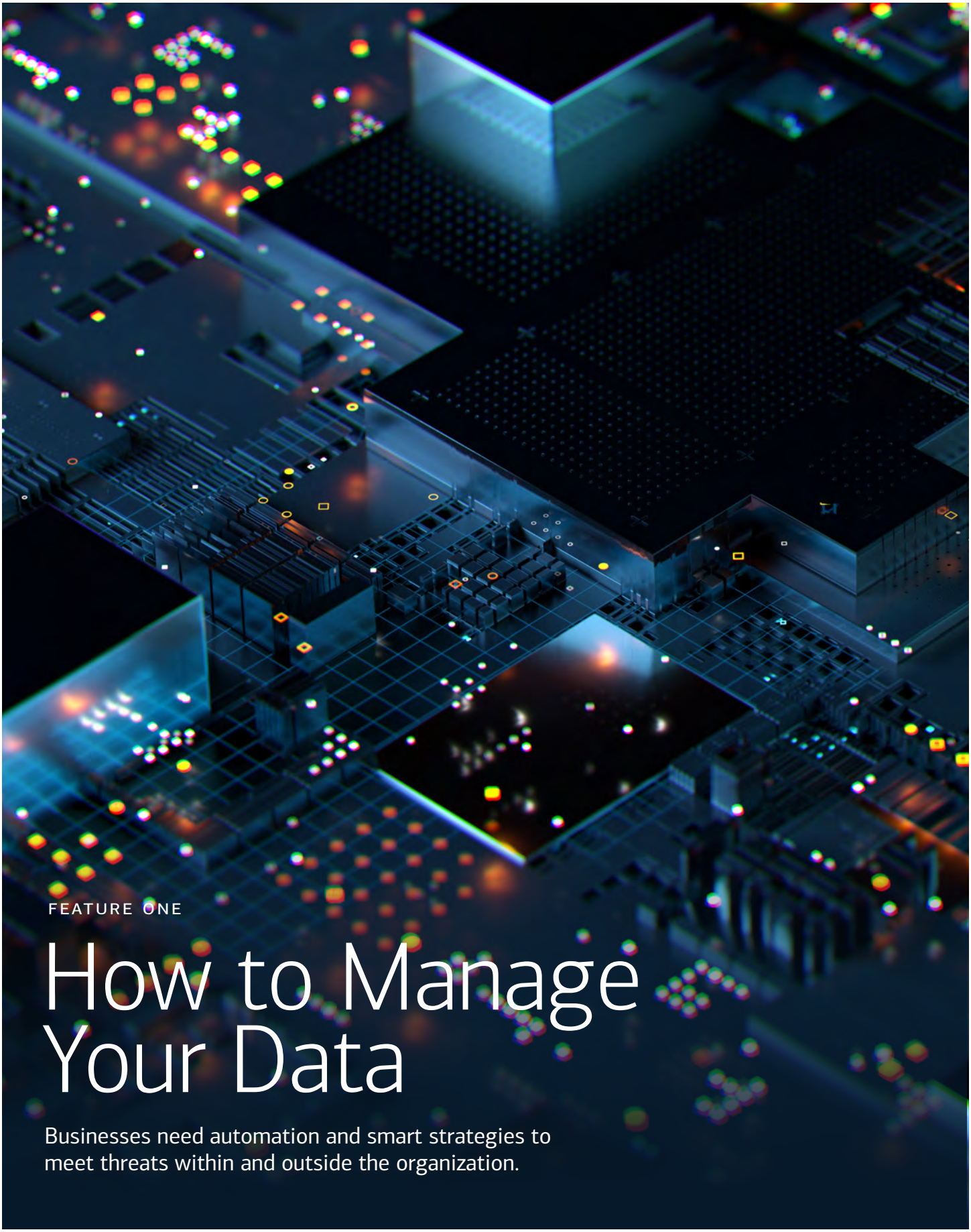
We're Dedicated to Protecting You Year-Round.

Craig Froelich

October is Cyber Security Awareness Month, and as part of our ongoing commitment to protect you, your business and the communities in which we operate, we are happy to share the third issue of our Cyber Security Journal. Helping you understand how to protect yourself and your company from cyber threats with the most current information available is one of our highest priorities, because your trust in us is essential to our business.

In this issue of our Cyber Security Journal, you will learn best practices for managing your data, access, and third party vendors. Mitigating risk, learning these best practices and implementing them are essential steps to ensuring your company remains cyber secure during Cyber Security Awareness Month and beyond.

Chief Information Security Officer, Bank of America

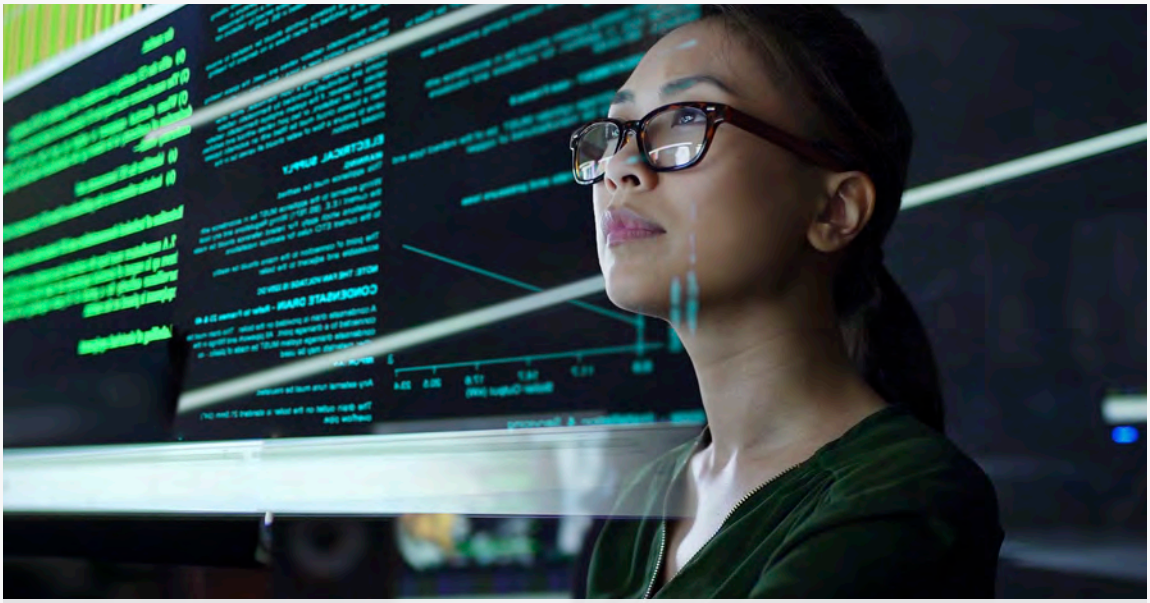


FEATURE ONE

How to Manage Your Data

Businesses need automation and smart strategies to meet threats within and outside the organization.

Data Theft



Data governance is a problem of growing complexity and importance in many industries.

Call it the data/security paradox. As the volume and complexity of data increases, the ability to secure this information decreases. The reason? Businesses are struggling under an unprecedented load of data that is difficult to manage — and to understand. Many businesses aren't fully aware of what data they have and where it's stored. The situation presents a basic tenet of cyber security in real time: You can't protect what you don't know.

To safeguard information, businesses need to be able to see their data across the ecosystem, which often includes external third parties and vendors. They need to identify the most sensitive information and determine where it should reside and who needs access to it. In many cases, businesses also need to make sure the storage and access to this data comply with industry regulations.

This knowledge is more important than ever, as remote working schedules have pushed the boundaries of the data ecosystem beyond the central-office perimeter. Taking work out of the office makes it much harder to monitor employee access and behavior. One recent survey found that 88% of U.S. businesses said coronavirus work-from-home mandates have increased the frequency of cyber incidents.[1]

At the same time, overall security risks continue to mount. Another study found that 59% of global organizations experienced a significant data breach within the last 12 months, a 9% increase over the year before.[2] (See page 8, "Data breaches by the numbers")

Detection and mitigation of these ramped-up risks require a data-governance framework that is unique to the organization. Data governance is a discipline that manages the quality and integrity of information to help ensure that data is reliable and trustworthy, while minimizing the risk of compromise.

Without a sound governing strategy, data management can become cumbersome, expensive or ineffective at mitigating the risk of data theft or loss. Finding the right solution is a formidable problem, but businesses that don't implement a strategy

"A successful data-governance program will require behavioral change from leadership. Buy-in must be top-down, not bottom-up."

Cyber Security Journal
Vol. One / Issue Three

Data governance often depends on integrating many disparate systems.

“Businesses must identify sensitive information, determine where it resides and who needs access to it and establish relevant regulatory obligations.”

must live with the increasing likelihood of breaches — and the financial and reputational impacts they can bring.

The benefits and challenges of data governance

Data governance is a work in progress for most companies and even technology experts. But the benefits of a strong framework are becoming clear. The right mix of technologies, processes and staff skills can strengthen cyber security, streamline operational processes and enable business leaders to make more informed, data-driven decisions.

As with most business priorities, good governance starts at the top. Leadership needs to recognize the value of its data and supply sufficient resources for a strong protective structure. This approach must involve more than greenlighting a technical solution. Decision makers need to understand the true benefit of generating, protecting and analyzing quality data. Smart data governance can deliver substantial cost savings to an organization, or potentially increase revenue through analytics and better competition strategies.

IT leaders should be prepared to deliver a persuasive, business-focused account of how governance can help balance security and data needs while reducing costs and boosting operational efficiency. If the rest of the company’s leadership doesn't see the intrinsic value or fails to provide oversight and top-down direction, a governance strategy is difficult to implement.

Smart governance strategies also depend on data centralization to help ensure that only the most accurate and relevant information is being used. Centralization allows businesses to more efficiently — and cost-effectively — process large volumes of data while deriving its maximum value. It also enables more informed, data-driven decisions based on consolidated information.

For instance, centralized governance can improve performance by identifying and mitigating redundant data and processes. Combined with redundant controls and user monitoring, this can eliminate single points of failure so that one mistake by an employee doesn’t result in a data compromise. If a breach does occur, governance can improve remediation time after an incident occurs.

But as with any complex initiative, strategy implementation presents a number of challenges. Since data governance is a relatively new discipline, many businesses lack the knowledge and resources to establish a multifaceted data framework. Doing so will require integration of multiple systems, processes and controls across IT areas and lines of business.

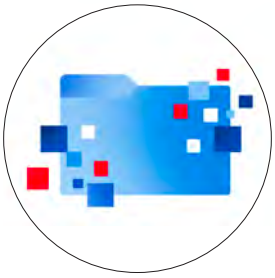
Effective data governance must also balance security and strong policies with ease of use to help support end-user acceptance. This is critical because, when faced with burdensome, repetitive security processes, employees may opt to bypass governance rules and set up their own shared drives or cloud applications. This behavior may not be intentionally criminal — most people

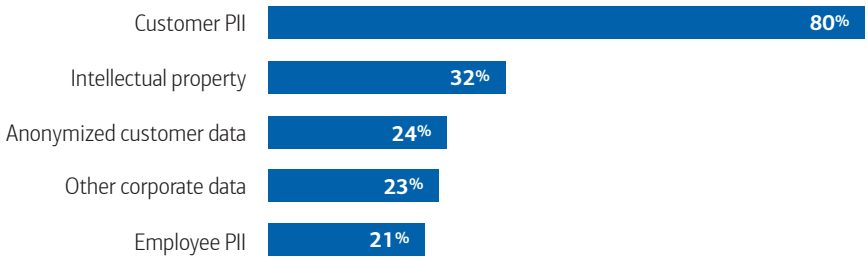
Continued on page 8

A snapshot of the threat landscape

As data becomes more valuable to the enterprise, opportunities for cyber criminals multiply. Research shows that customer data is most at risk, but corporate-data and intellectual-property theft are growing concerns.

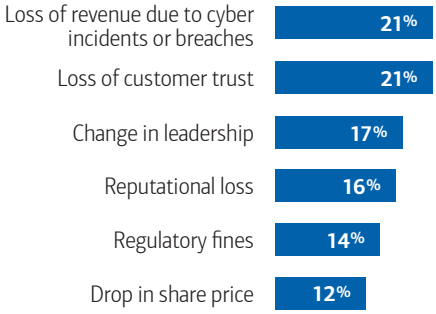
Types of records compromised:





Source: Ponemon Institute, Cost of Data Breach Report 2020, July 2020

Biggest impacts of incidents and breaches:



Source: Deloitte, The Future of Cyber Survey 2019, March 2019

Threat actors responsibe for incidents:

Source: EY, Global Information Security Survey 2020, February 2020

Data breaches by the numbers:

59%
of organizations experienced a significant or material breach in 2019, a 9% increase over the year before.[1]

91%
of global businesses report an increase in overall cyber security compromises as a result of employees working from home.[2]

$8.6 million
Average total cost of a data breach in the U.S. (the highest of any country).[3]

$2.45 million
Average 2020 cost of a data breach for companies with fully deployed security automation.[4]

$6 million
Average 2020 cost of a data breach for companies that had not deployed security automation.[5]

[1] *EY, Global Information Security Survey 2020, February 2020.*

[2] *VMWare and Carbon Black, Global Threat Report: Extended enterprise under threat, June 2020.*

[3] *Ponemon Institute, Cost of a Data Breach Report 2020, July 2020.*

[4,5] *Ibid.*

Vendors and third parties can complement — or compromise — a sound data-governance strategy.

Continued from page 6

are just trying to get their jobs done, after all — but it can result in unnecessarily risky compromises.

One often-overlooked risk is the security profile and capacity of third-party partners that have access to their clients' data, networks or applications. Companies will need to determine whether external partners have established security and privacy protections robust enough to protect and verify their data. And it's important to remember that *company* data is *the company's* responsibility, no matter where that information resides. This accountability cannot be offloaded to third-party partners or cloud providers.

Automated tools provide valuable assists

More than ever, effective data governance relies on technologies to automate processes and gain a deeper understanding of data. These tools include data classification, data-loss prevention (DLP) and machine learning.

A foundational component of governance is data classification, which organizes information into categories — such as "sensitive," "regulated" and "intellectual property" — to help businesses more efficiently process and protect information. Data classification can also help speed up the detection and mitigation of breaches, which can deliver cost savings. Another critical consideration is data verification, which assesses data for accuracy.

When it comes to managing internal threats, DLP can be especially valuable. This is an approach to protecting data that uses policies, processes and technology controls to protect data in its various states (in use, in motion and at rest). DLP allows businesses to monitor user behavior to detect internal risks as well as unintentional data loss by insiders who transmit sensitive information to external networks and recipients.

“New machine-learning tooling has become a game changer in the identification element of data control. With machine learning, a business can define the rules and the technology will classify the data.”

DLP has become even more critical as many employees continue to work from home. Based on predefined rules, DLP tools can scan emails to identify restricted information like credit-card or Social Security numbers. If such information is detected, DLP tools can bar transmission of this data outside the corporate network.

Another technology trend among forward-thinking businesses is the use of machine learning (ML) to manage data. ML enables companies to establish data-classification rules and use automated processes to identify and classify information across the enterprise. This type of process automation can allow businesses to more quickly and cost-effectively identify and contain breaches. In fact, process automation helped trim the time it takes to identify and contain breaches from an average of 280 days to 206 days — with an average savings of $3.58 million, according to a 2020 study by the Ponemon Institute.[3]

Automated processes can reduce the risk of data loss or theft.

Governance strategies still rely on people

More than ever, employee security awareness and training on current threats and their potential impacts remain the most effective, inexpensive way to curb data loss. It’s particularly important to communicate the potential real-world impact of breaches on business performance and data security. Doing so will drive home the consequences of disregarding new security processes and help ensure the success of a data-protection program.

Also critical is effective communication about data-protection programs. Businesses must clearly convey to employees why data governance is a fundamental — and increasingly urgent — business requirement, and how it syncs with regulatory obligations.

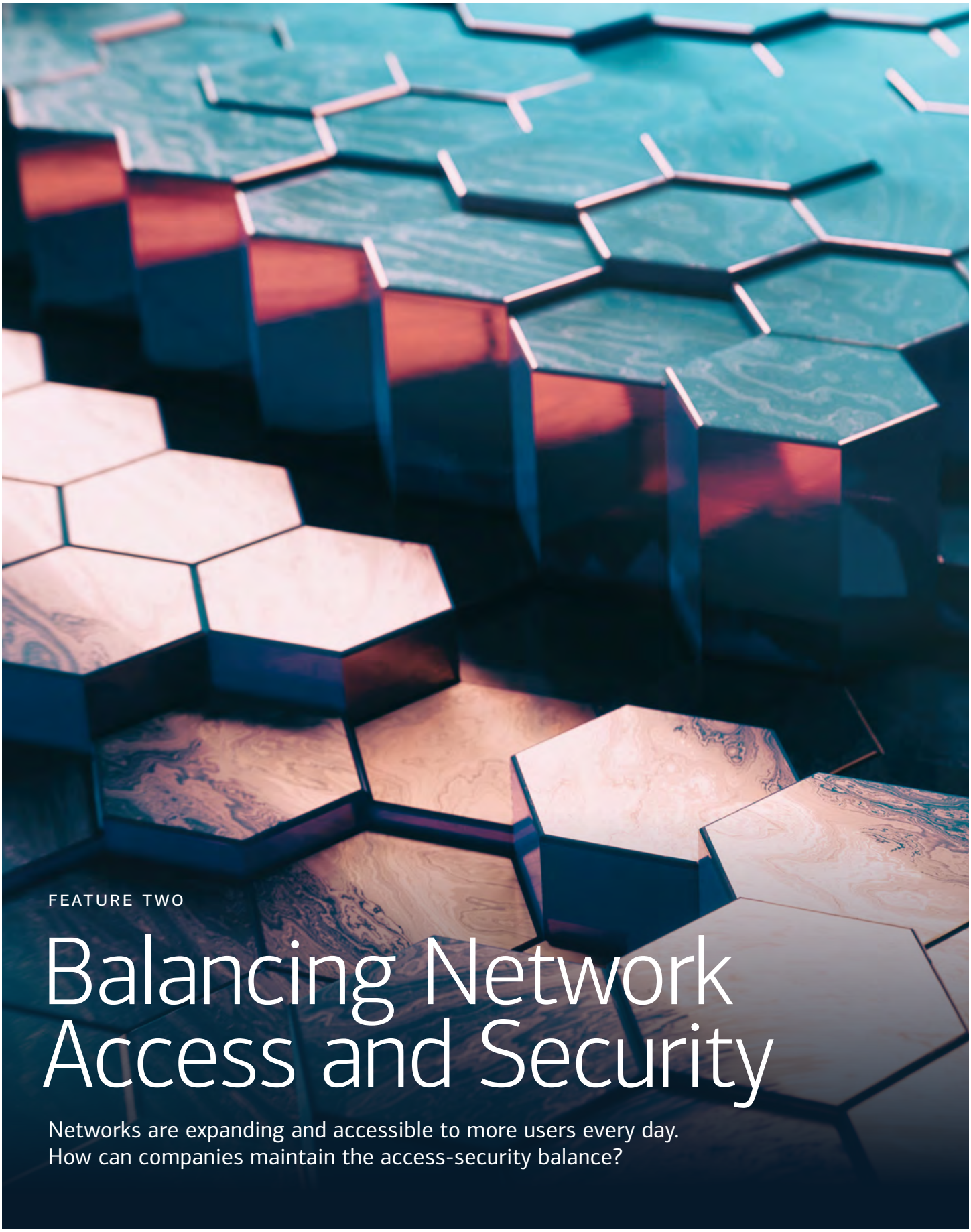
Developing a data-governance strategy can seem overwhelming to those with limited experience classifying and aligning data with cyber security programs. But businesses can realize gains by taking small steps to design a program, classify and verify data and configure a robust DLP solution. Doing so will help safeguard the business, as well as its data and employees. ■

Data Theft

Key takeaways:

- Understanding the variety of data a company possesses, and where it’s stored, is the fundamental first step of loss and theft prevention.
- Protecting data requires a careful consideration of potential insider threats as well as strong defenses against cyber crime.
- Strong governance and automated processes can help contain the damage from breaches, but training and active monitoring are also essential practices in data governance.

[1] *VMWare, Global Threat Report: Extended Enterprise Under Threat, June 2020.*
[2] *EY, Global Information Security Survey 2020, February 2020.*
[3] *Ponemon Institute, Cost of a Data Breach Report 2020, July 2020.*

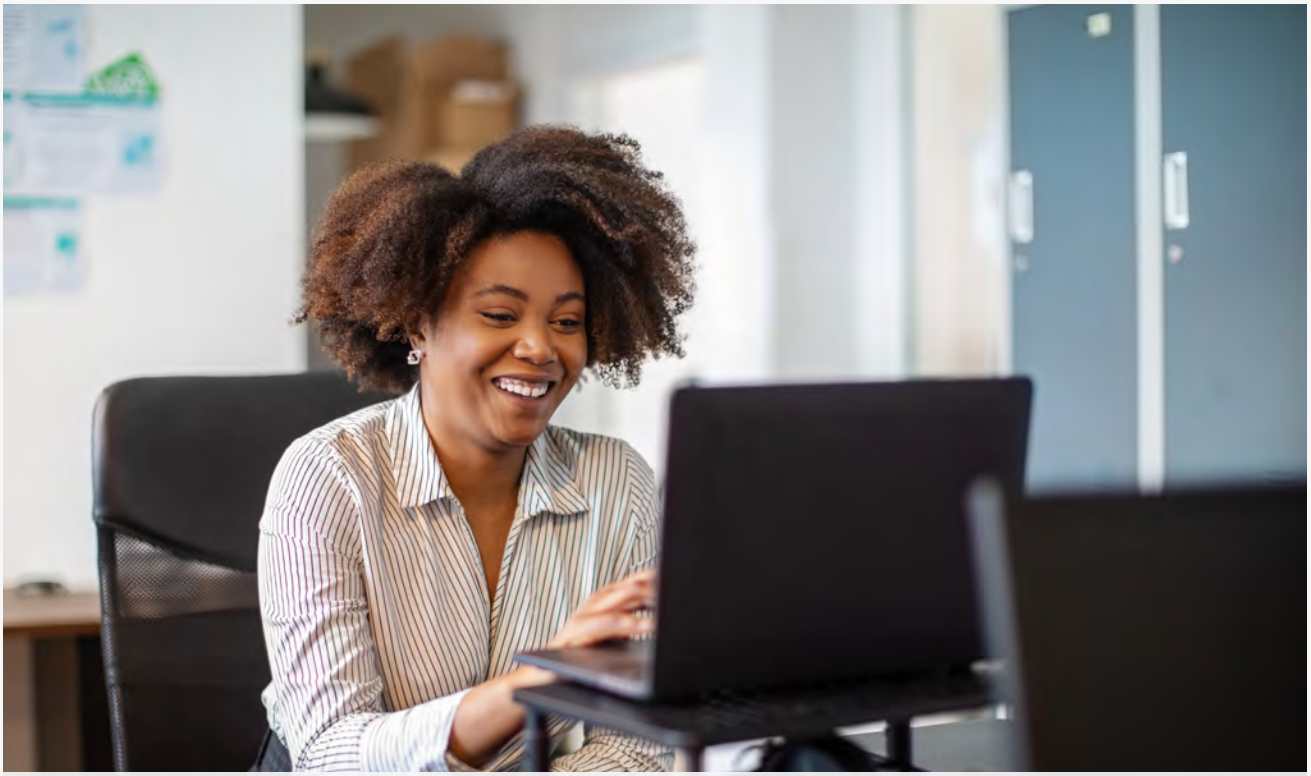


FEATURE TWO

Balancing Network Access and Security

Networks are expanding and accessible to more users every day. How can companies maintain the access-security balance?

Access Management



Access management now depends on continuous monitoring, rather than simply granting or denying user privileges.

Gone are the days in which usernames and passwords were enough to verify identity and control access to key systems and data.

The security boundaries of today's organizations are complex and evolving. Controlling access to them is no longer a yes-or-no proposition. Instead, companies must continuously monitor the behaviors and patterns of access within their networks and become smarter about how they set up access privileges in the first place.

In today's globally connected, digitally driven economy, the "threat surfaces" of systems, tools and databases of most organizations are expanding. This means the number of information systems that require administration of user access is also increasing rapidly. To keep pace with the change, many companies are embracing an enterprise-resource-planning (ERP) model that abandons traditional, monolithic software suites in favor of a modular approach using diverse, cloud-based vendors.

This so-called postmodern ERP leads to users' accessing data through multiple channels — and also opens up more avenues for fraudulent access. In addition, by shifting workloads to the cloud and outside the enterprise perimeter, businesses lose controls that internal IT processes would traditionally apply. Without sufficient controls, cyber threats can quickly increase.

On top of that, the number of access points to a company's networks is multiplying every day — whether it's users, devices or APIs. The growth is accelerated by the proliferation of connected devices, the steady move to cloud computing and the dramatic increase in remote and mobile access during the coronavirus pandemic.

Inadequate or complicated access to business systems is more than a headache. It can damage a company's bottom line if users can't fulfill their business responsibilities in a timely and efficient manner. Too much unregulated access, however, can present a serious cyber security hazard. When workers

have more privileges than they need, there is increased risk from external threat actors attempting to compromise accounts. Un- or under-regulated access also increases the risk of insider threats, which might include intentional fraud, theft or inadvertent mistakes, such as wiping out or corrupting large quantities of data.

A competitive balance between access and security is still possible. But decision makers must recognize how the access-management equation continues to change.

Interconnected networks complicate issues of access, privilege and risk.

Understanding risk-appropriate access

How can companies stay safe while not overburdening employees with overly complex protections? The answer may be through a concept known as the principle of least privilege: provide users, programs or processes with the minimum privileges necessary to perform a function.

This approach grants access based on user identity, the role of the user within the organization and what information or tools they need to do their job. Risk is then evaluated end to end, from the point at which the user is authenticated and through to access administration.

In addition, companies can enforce segregation of duties (SoD), a process in which responsibilities for key processes are divided between more than one person. This can keep users from assuming excessive privileges that might allow them to circumvent normal controls — and exploit them to enrich themselves or make unchecked mistakes.

If a user needs elevated privileges (i.e., a higher level of access such as that of an administrator), those privileges need to be carefully monitored, and possibly time-bound, so users don't have the elevated privileges perpetually.

Most importantly, companies should always think in terms of resiliency. While it's impossible to prevent every risk, being in a position to recognize when a problem occurs and recovering quickly can dramatically reduce damage.

Access management as a four-pillared business practice

Strategic access control is critical to preventing cyber security breaches, but it should enhance overall productivity and flexibility, not hinder them. In the best circumstance, access management will combine sound poli-

Access-management glossary

Elevated privilege — A higher level of access to systems and resources, such as that of an administrator.

Excessive privilege — More access privileges than the user needs to perform their duties.

Least privilege — The principle of giving users, programs or processes the minimum privileges necessary to perform a function.

Risk-appropriate access — Access based on the evaluation of end-to-end risk, considering user identity, roles the user performs in the organization and what they need to perform their duties.

Segregation of duties (SoD) — The division of responsibilities for key processes between more than one person in order to prevent fraud and error.

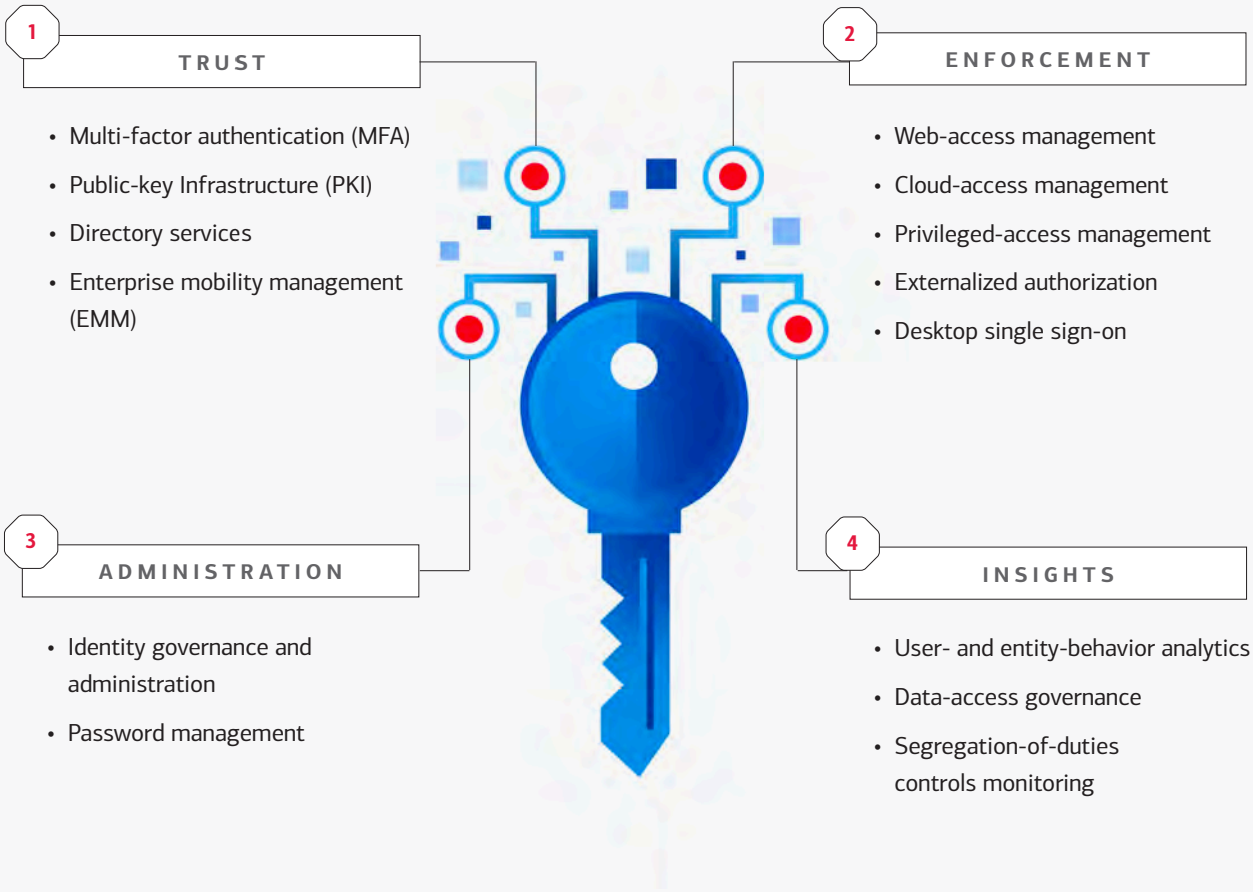
cies, controls and systems and address a variety of business issues that are impacted by identity and access.

By examining their needs and current maturity within a framework of four pillars — trust, enforcement, administration and insights — businesses can begin to develop an access management strategy that will match their specific requirements.

Trust deals with the primary challenge of access management: How can a company confirm that a person is who they say they are and that any system they're using is what it's advertised to be? Using multi-factor authentication to verify identity with several pieces of evidence (e.g., something the user knows and something the user has) is just the first step. Public-key infrastructure (PKI) helps encrypt communications with the use of digital signatures and certificates. Enterprise mobility management (EMM) protects company data on mobile devices, which is especially critical as more employees demand bring-your-own-device (BYOD) policies. PKI and EMM are becoming increasingly common

Four pillars of access management

Companies can protect the ever-expanding surface of their networks through a four-point strategy that may deploy a wide variety of tools and processes:



parts of a protective infrastructure along with software tools such as directory services, which can help create a map of user access behavior throughout network resources.

Enforcement tools can help an organization ensure that its access-control policies are in place throughout a varied network ecosystem. These may include access management for web servers, cloud platforms and applications. Applying principles such as least privilege and implementing privileged-access management tools to control elevated access can help enforce threat-mitigation policies. And processes such as single sign-on (SSO) also support enforcement operations by improving identity protection while delivering a streamlined user experience that enhances security compliance.

Access management strategies can streamline connections between legacy systems.

Administration tools leverage automation to streamline permissions and password management. With multiple legacy systems providing their own user accounts and permissions, companies need methods to seamlessly administer them all. This may include identity governance and administration tools to provide policy-based rules for user-identity management and access control, as well as tools for automated storage, management and protection of passwords.

Finally, regular review of established access-management processes can generate valuable insights into an organization's operations and efficiencies. Businesses ready for a more mature access-management strategy can leverage a variety of tools that examine user behavior for patterns and characterize critical data sets.

User- and entity-behavior analytics (UEBA), for example, use machine learning to identify anomalous patterns that could be a sign of a cyber breach. Perhaps even more importantly, data-access governance can help companies gain visibility into sensitive unstructured data and enforce policies to control ac-

"Analysis of access patterns and data flows can detect anomalous behavior and help the organization locate its most sensitive and valuable data."

The changing landscape of network access:

54%

Percentage of organizations that required remote work in response to COVID-19.

76%

Percentage of organizations reporting that remote work would increase time to identify and contain a data breach.

70%

Percentage of organizations reporting that remote work would increase the cost of a data breach.[1]

[1] *All statistics from IBM Security, "The Cost of a Data Breach 2020."*

Cyber Security Journal
Vol. One / Issue Three

Smart access-management strategies should support intuitive approaches to work.

Access Management

Key takeaways:

- Continuously monitoring behaviors and patterns of access within networks can help ensure that every user, device and API has the appropriate level of access to the right resources.
- The principle of least privilege, which provides users, programs or processes with the minimum privileges necessary to perform a function can often be foundational to company access-management strategies.
- Examining business needs and maturity against the framework of Trust, Enforcement, Administration and Insights can help develop a balanced access-management strategy.

cess to that data. Continuously analyzing access patterns and critical data, as well as monitoring SoD risks, can provide organizations clearer visibility into where its sensitive data resides and who has access to it.

Practicing access management is an art, not a science

Ultimately, companies can benefit from a balanced approach that assesses the strength of the four pillars and allocates investment across them according to need. For instance, functional trust and enforcement capabilities depend on a viable administrative capability. But a company shouldn't focus only on getting administration capabilities completely up and running before it invests in trust and en-forcement. Each pillar must be robust for comprehensive and reliably safe access management.

The goal is to gain deeper insight into data and transactions while keeping access-management protocols strong. By mapping data to transactions, for example, capabilities like data-access governance, monitoring and entity-behavior analytics can produce a clearer picture — and therefore better control over — who has access to what. ■

FEATURE THREE

The Science of Managing Third Parties

Many companies depend on vendors for support with client and employee business needs. How can they determine these partnerships are cyber-secure?

Third-Party Management

As business services and operations automate and go online — into the cloud and onto mobile devices — many companies recognize that their prosperity depends on sophisticated digital workflows and capabilities. This means they also rely on an ever-expanding pool of experts who can maintain and monitor every facet of their business and customer interactions.

Most companies can't hire all the in-house specialists they need to be competitive. This means outside vendors are playing an expanding role in their organizations, including information-technology (IT) functions. Even as digital functionality and automation improve services such as benefits, payroll or cloud services, there is a pressing need for rigorous human oversight and specialized operations maintenance.

There are many types of vendors and software platforms that can handle tasks that a company chooses to outsource. However, given their connections to critical industries, it is hardly surprising that these same service providers have become targets for cyber criminals and potential jumping-off points for attempts to breach the networks of companies they serve.

Fortunately, there are ways for companies to evaluate any potential or existing relationships with third-party vendors. The better companies understand their own cyber security risks and workflows, the better equipped they are to evaluate the complex services market and establish partnerships that maintain stability and enhance growth opportunities in a secure manner.

But companies also need to understand how vendors function and respond to emerging threats to their customers — as well as to themselves. Whether these vendors are managing social media, communications, cloud functionality, payroll, accounting services, cyber security or any other essential function, they will need access to some or all of their clients' most important systems and data.

Standards for these outsourcing arrangements must be kept high. Security breaches, service interruptions, regulatory violations, insider threats and reputational damage can be the result if a company has engaged a vendor that is a mismatch or doesn't maintain appropriate controls or standards.

Cloud and other technologies are changing how third parties operate.

The fundamentals are not a third party's job

As data becomes more specialized and valuable, and regulations change how companies operate, any outside vendor will need to know something about how their potential customer prioritizes data and intends to use it. But that analysis can't begin with the

"Businesses of all types are relying on third-party services to stay competitive, but many are worried about the security risks that accompany these relationships."

service provider: Company decision makers need to assess their needs and risks carefully before they outsource. That requires a meticulous review of people and policies, as well as technology.

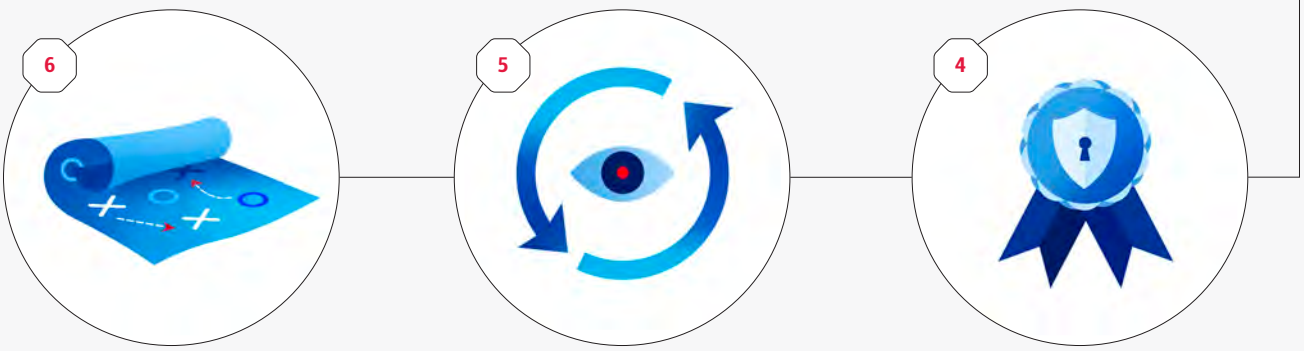
Before discussions with any vendor begin, a business should have a clear sense of how and where its data flows; what regulatory conditions apply; what people, policies and technologies currently protect the data; and how it can be recovered in the event of downtime or a breach. This analysis may seem rudimentary, but the point is that such due diligence can't be offloaded to a third-party provider, no matter how impressive its reputation or capabilities may be.

Before selecting any vendor, a company should also gauge the acceptable

How can you evaluate a vendor's approach to cyber security?

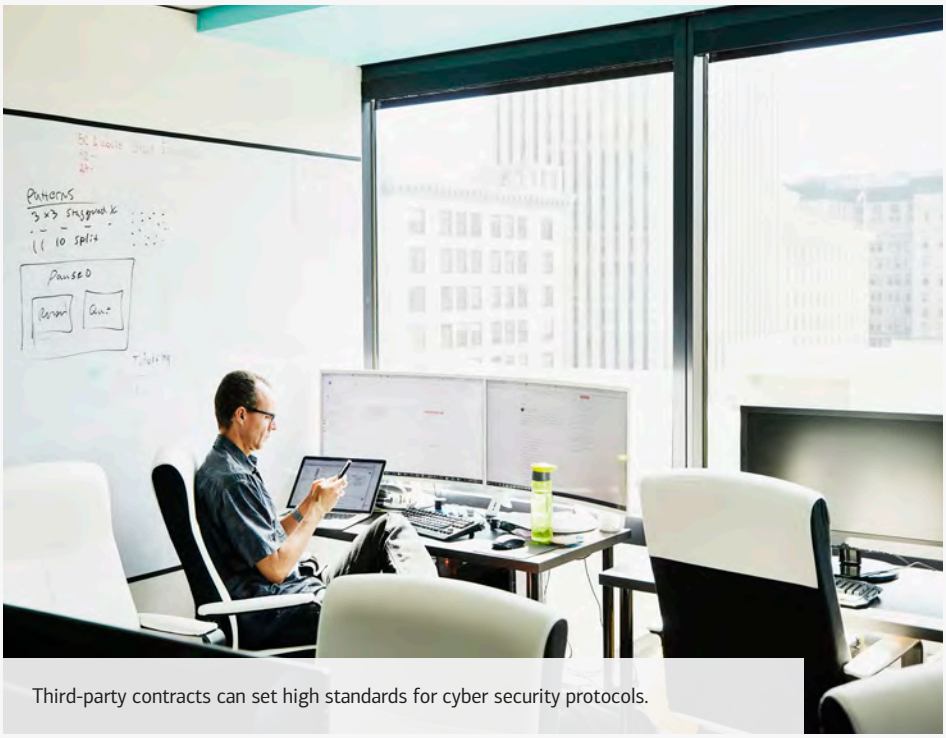
There is no one right way to evaluate the capabilities of a service provider or the quality of an existing service contract. Decision makers can evaluate the quality of a vendor's operations with a variety of metrics:

- **Party-to-party risk review.** The vendor should regularly update its clients about internal risk assessments and remediation plans.
- **Independent review.** Reports conducted by outside parties, such as the American Institute of CPAs, can establish that vendors are operating at high standards of trust and service.
- **Automated reporting.** Companies may receive real-time reports based on measurement of key vendor operations.



- **Remediation planning.** An emergency-response plan should be available and adaptable to the client's specifications.
- **Responsiveness.** Vendors should be able to demonstrate a record of availability and timely alerts.
- **Education.** Third parties should demonstrate regular training and cyber security awareness-building for their employees.

Illustration by Jack Hudson



Third-party contracts can set high standards for cyber security protocols.

“Service contracts should require regular risk review, monitoring and remediation plans of most third-party service providers.”

risk the partnership presents. For those vendors who will handle the most sensitive or valuable data — or have frequent access to the networks, and thus present the greatest risk — the standards for selection and management must be robust and adaptable.

Set the terms of service and security

As data becomes more valuable and third-party security breaches more common, the stakes for finding the right business partnerships are only increasing. How can companies determine that these partnerships will deliver what they promise and that the vendor’s internal security controls are robust? What approach can confirm that a vendor is maintaining its standards and evolving to meet new security requirements?

A detailed service contract that speaks to the company’s requirements and risks can provide a protective framework for the relationship. Before any agreement is signed, the company needs to ask questions about risk within the vendor’s environment and make sure that regular review and reporting will be a part of the core service.

Contracts also can implement key performance indicators (KPIs) that align with the outsourcing company’s risk tolerance, best practices around network testing, incident-response protocols and employee access-management controls, to name just a few potential conditions. Since technology improvements can be expensive or create a disruption in company operation or income generation, it also should be clear which party will be responsible for upgrade costs.

All contracts should reflect the organization’s risk tolerance and security concerns. They also can set the parameters for ongoing review by requiring the vendor to maintain regular testing of their networks and security training for employees. These measures can help a company understand how the vendor approaches cyber security and set benchmarks for responsiveness and operations maintenance.

Maintain vigilance through compliance and ongoing review

At a time when more workers than ever are remote, utilizing cloud capabilities and networks of connected devices, third-party management is facing new complications.

Cyber Security Journal
Vol. One / Issue Three

A growing market — and growing risk

Businesses are more reliant on outsourced services than ever before. But the risk associated with the convenience is also on the rise:

$270 billion

Estimated worldwide revenue of business-process outsourcing, 2020.[1]

$382 billion

Estimated worldwide revenue of business-process outsourcing, 2025.[2]

84%

Percentage of surveyed companies that experienced a third-party risk incident in the last three years.[3]

17%

Percentage of surveyed companies that experienced a high-impact risk incident through a third party in the last three years.[4]

46%

Percentage of surveyed companies that outsource more than 50% of their digital operations to third parties.[5]

[1] *Statista, Technology Market Outlook, Business Process Outsourcing, 2020.*
[2] *Ibid.*
[3] *Deloitte, "Third-party risk management (TPRM) global survey, 2020."*
[4] *Ibid.*
[5] *Deloitte, "The Future of Cyber Survey," 2019.*

Independent review may be essential in the most critical third-party relationships.

As companies change the way they work, they must be sure vendors are responsive to emerging threats and are not introducing new vulnerabilities to the existing relationship.

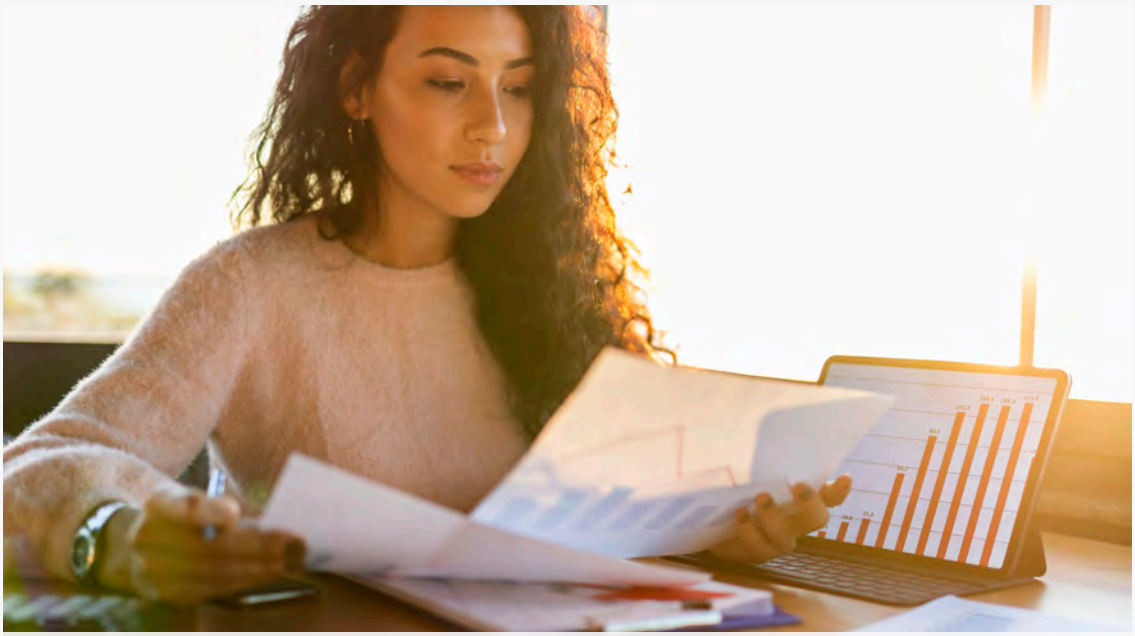
Independent reports on a vendor's practices can provide an extra layer of oversight. Such review can generate a nuanced assessment that focuses on trustworthiness and diligence, and it may be a smart addition to large and ongoing service contracts. These reports can be expensive, however, and it may be unrealistic to expect smaller service providers to assume the cost just to satisfy the expectations of one client.

Some companies may ask their vendors to comply with remote audits of their key services to ensure compliance. Others may request automated reports that are generated when certain risk metrics or thresholds are passed. Those with more advanced capabilities may request the vendor adopt certain controls to enable more real-time monitoring.

But as with any other element of digital operations, even automated tools are of limited efficiency if the people deploying them are not responsive. A vendor that complies with a company's security requests and submits regular reports may still be ineffective if it does not make cyber security

"Prioritizing company data, and understanding where it lives, is essential to managing third-party risk."

Cyber Security Journal
Vol. One / Issue Three



Companies that prioritize cyber security should seek vendors that strive for similarly high standards of protection and awareness.

an organizationwide priority.

In an emergency, the most reliable quality indicators may be whether or not the vendor immediately picks up a distress call and rolls out a comprehensive, effective response. But companies can gauge that responsiveness by asking the vendor in advance about its backup and remedial procedures in the event of a systems failure or security breach.

Strong client-facing skills still matter

Ultimately, decision makers can narrow their search for the right third-party service provider by looking first for subtle, people-oriented skills. Any vendor that touches a company's networks and most valuable data will need to demonstrate trustworthiness, a willingness to understand a client's unique needs and accountability in terms of contracts and reputation.

Companies that take cyber security seriously and implement strong, adaptive protocols can leverage their smart approach in third-party contracts. The higher your own security and operational standards are, the more you can expect out of any vendor relationship. ■

"A third party's protections and protocols will only be as strong as the people who maintain its operations and client services."

Third-Party Management

Key takeaways:

- Risk review of a contract with any service provider can be easier and more effective if internal risk assessments are thorough and based on strong protocols.
- In a rapidly changing landscape, third-party management increasingly relies on monitoring and regular reporting.
- Responsiveness and planning can be just as critical as technological expertise when companies outsource some or all of their operations to third parties.