WHITE PAPER

PROTECTING DATA IN A SHIFTING SECURITY LANDSCAPE

As threats evolve, new strategies and solutions can help organizations safeguard their data.

EXECUTIVE SUMMARY

Organizations in every industry have long understood the importance of data protection. But the task for many has been too much to handle, and as security threats have evolved, organizations have struggled to keep up.

Only a few years ago, ensuring data safety mostly came down to defense of the network perimeter. With a correctly configured firewall fortified with regular updates, a trained IT professional could successfully repel most cyberattacks. But the risks to data today are of a vastly different sort, and the threats that organizations face are more frequent and dangerous. With the Internet of Things (IoT), the cloud and artificial intelligence in play — and the volume of vulnerable data expanding exponentially — to simply rely on a network barrier is no longer good enough.

The answer instead, experts agree, is to implement a multifaceted cybersecurity program that takes an adaptable approach to preventing, containing and remediating attacks. As cybercriminals look to new and increasingly sophisticated ways to infiltrate the systems organizations have in place, there's no way to avoid every possible threat. But, equipped with the right tools and supported with the right services, organizations can manage the threats they do face — and, ultimately, they can make data protection a reality.

A Shifting Data Security Landscape

The root of the data security problem for most organizations has everything to do with changing technologies combined with the sheer volume of data now at stake. Digital transformation across industries in recent years has helped drive significant improvements in business management and workflows, but it has also made organizations of all sizes vulnerable to many new and shifting threats. As an enterprise expands the number of devices it has in service, and as more of these technologies become digitally connected, the chance that they will experience security issues increases as well — often in ways that are difficult to predict.

One recent report by the market intelligence firm IDC, "The Digitization of the World from Edge to Core," predicts that the total volume of data worldwide will increase from 33 zettabytes (one zettabyte equals a trillion gigabytes) in 2018 to 175ZB in 2025. Over the next five years, IDC forecasts, the IoT will expand to include more than 150 billion connected devices. Data "is at the heart of digital transformation," the report notes, and enterprises are using it "to improve customer experiences, open new markets, make employees and processes more productive, and create new sources of competitive advantage."

The primary data-related challenge for these organizations involves its continuous management: As companies adopt digital technologies to bolster efficiencies and business intelligence, they have to ensure they can keep these systems safe from the cybercriminals who see them as their personal pots of gold. Digital innovation, notes a report from Microsoft and Marsh & McLennan ("2019 Global Cyber Risk Perception Survey"), is critical to success for most businesses, but it also "often adds to the complexity of an organization's technology footprint, including its cyber risk." When Microsoft and Marsh polled 1,500 business leaders around the world, 79 percent of respondents ranked cyber risk among the five most significant concerns for their organization, and many indicated they worried that they lacked the ability to manage such risks. According to the survey, 18 percent of respondents said they had "no confidence" their organization was capable of understanding and assessing cyber risks; 19 percent said they didn't believe their organization could prevent cyberattacks; and 22 percent indicated they lacked the ability to respond to and recover from cyber events.

279
DAYS
The average amount of time needed to detect and contain a cybersecurity breach[1]

New Cyber Risks, New Threats to Data

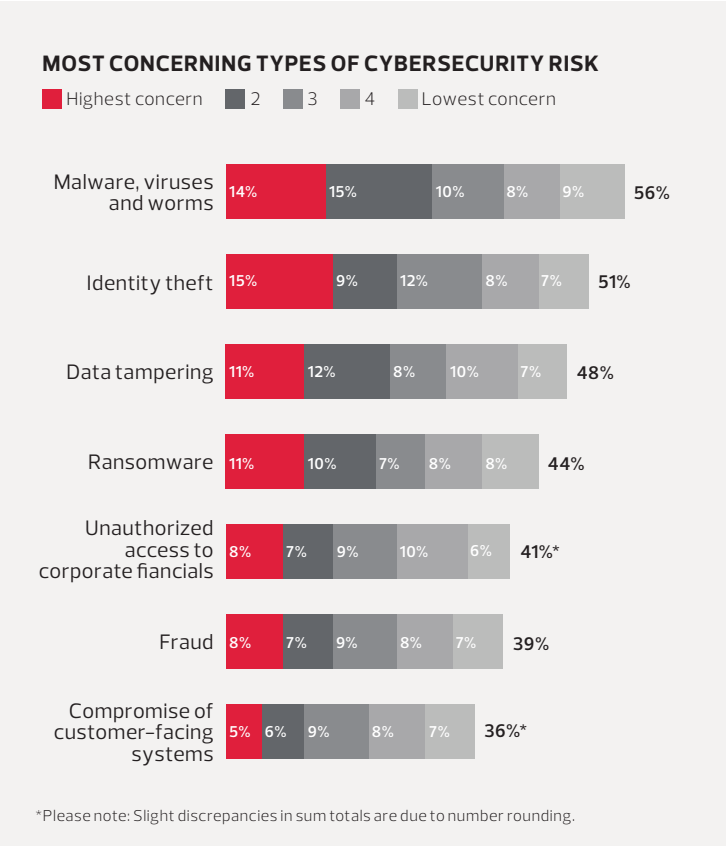
So, what cyber risks do organizations actually face? On a macro level, according to another recent survey — "State of Enterprise Risk Management 2020," by the IT governance association ISACA, the CMMI Institute and Infosecurity Group — organizations report that the biggest threats to cybersecurity include "changes/advances in technology" (64 percent), "changes in the types of threats" (60 percent), "too few security personnel" (52 percent), "missing skills in existing cybersecurity team personnel" (51 percent) and "increased number of threats and/or increased frequency of threat occurrence" (45 percent).

But the specific lines of attack vary significantly. For example, many cybercriminals exploit frontline employees through social engineering to gain access to an organization's information systems. Phishing attacks that use phony email to exploit users and steal their login credentials are also common. Another common attack vector is malware (including mobile malware), delivered via email as an image, a PDF or a link to a malicious website. And with many attacks, there's the added threat that the infiltration may go undetected for an extended period. Median "dwell time," as it's known, has decreased, thanks in part to better awareness of cybercrime and new detection technologies. But as any company that has a cybercriminal who has been prowling through its systems unnoticed will attest, a dwell time of any length is far too long.

Source: [1]Ponemon Institute, "2019 Cost of a Data Breach Report," July 2019

Once a cybercriminal has access to an organization's systems, anything could happen next. A company hit with encryption ransomware might find it impossible to access important files unless it pays a substantial fee in cryptocurrency to the attacker. Or the cybercriminal might threaten to publicize sensitive data and expose the company in ways that could damage its reputation. A malware infection on the systems of a major retailer could lead to the exposure of customer credit card accounts, while a similar attack on the financial systems of a university might threaten the private data of faculty and students. A 2019 IDG Research/CDW survey of more than 400 IT professionals and business executives at companies with 250 or more employees asked participants to rank the specific cybersecurity risks that concerned them the most. Malware, viruses and worms were at the top of their list, followed by identify theft, data tampering and ransomware. Slightly less concerning to those who were polled: a slew of other potentially ruinous cybercrimes, including unauthorized access to corporate financials, network denial of service and espionage access to trade secrets.

Finally, many within the information security community believe that artificial intelligence is poised to revolutionize how cybercriminals work. Cyberattackers, explains an October 2019 article on the information security website Dark Reading, can use AI and deep learning to create "deepfakes," for example, where a person's voice or image is superimposed over another's to trick the listener or viewer into doing something against his or her interest. The author cites one instance where a cybercriminal used AI to dupe an energy business executive into wiring $243,000 to a company that didn't exist.



*Please note: Slight discrepancies in sum totals are due to number rounding.

It's the potential financial impact of cybercrime, in fact — and the fear that a breach may go uncontained to the point where the damage becomes irreversible — that keeps many IT professionals up at night. According to the Ponemon Institute's "2019 Cost of a Data Breach Report," the average data breach lifecycle — the time it takes for an organization to identify and contain a breach — rose 4.9 percent between 2018 and 2019, and is now up to 279 days. (That figure is for breaches of all kinds, including those that are criminal in nature and those that occur accidentally. In the case of criminal attacks, which are responsible for more than half of all breaches, the data breach lifecycle is now 314 days.) Longer breach lifecycles, the Ponemon report notes, inevitably lead to higher costs. The average total cost of a breach in 2019 was $3.9 million among organizations worldwide.

Developing a Strategy for Effective Data Security

Given the potential costs associated with a data breach, most organizations accept that it's imperative they invest in an effective cybersecurity plan. According to CIO magazine's "2019 State of the CIO" survey, the average organization now spends 15 percent of its total IT budget on cybersecurity. Other research, by IDG, found that 50 percent of organizations are planning to increase their security budgets over the next 12 months, and that many are "actively researching" zero-trust technologies (47 percent), deception technology (40 percent) and behavior monitoring and analysis capabilities (39 percent) to see how they might fit into a revamped data security strategy.

The exact steps involved in developing such a strategy are usually determined by the specific needs of the organization, but many organizations begin with guidance from the National Institute of Standards and Technology. NIST's Cybersecurity Framework, a set of standards, guidelines and practices designed to help organizations manage and reduce cybersecurity risks, includes details on what the institute describes as the five primary functions of any strong cybersecurity plan: **Identify, Protect, Detect, Respond and Recover**.

Identify

The first function, according to NIST, "assists in developing an organizational understanding to managing cybersecurity risk to systems, people, assets, data and capabilities." By conducting a risk assessment at the start — and looking closely at its current security posture — an organization can pinpoint the critical areas on which to focus when it's ready to implement new data protection solutions and services. Also known as a cybersecurity gap analysis, the process is designed to determine exactly how far an organization has to go to reach an optimal state of information security.

Protect

The next framework function involves the implementation of "appropriate safeguards to ensure delivery of critical infrastructure services." If and when a cyberattack occurs, the

protections an organization has in place should either be able to deter it altogether, or at least minimize its impact. Among the steps an enterprise can take to make protection a reality:

- **Establish protections** for identity management and access control, including physical and remote access.
- **Educate staff** in cybersecurity best practices with role-based and privileged-user training.
- **Implement security processes and procedures.**

Overcoming the Security Skills Shortage

It's no secret that industries everywhere are struggling to find IT professionals with cybersecurity training. The cybersecurity skills shortage is one of the biggest challenges organizations face as they look to improve data protection in an environment where threats are growing by the day.

"The cybersecurity skills shortage," notes a 2019 report from the Information Systems Security Association International, "continues to be the root cause of rising security incidents, as organizations remain plagued by a lack of end-user cybersecurity awareness and the inability to keep up with the growing cybersecurity workload."

According to the latest "Cybersecurity Workforce Study," an annual survey conducted by the International Information System Security Certification Consortium, there are now an estimated 4 million unfilled IT security positions at organizations worldwide. In the United States, the report notes, the "cybersecurity workforce gap" stands at about 500,000, which means the cybersecurity workforce needs to grow by 62 percent just to meet U.S. industry demand.

What can organizations do to make up for this deficiency? One possible answer, according to another recent study (conducted by the Ponemon Institute and DomainTools), involves accelerated adoption of automated cybersecurity technologies, including those that employ artificial intelligence. The study's authors note that automation can "improve teams' abilities to prioritize threats and vulnerabilities and increase the speed of analyzing them." The survey of more than 1,400 IT security professionals found that 79 percent of those in the United States have either already incorporated automation into their cybersecurity strategy or are planning to do so in the next three years. It also found that AI "is now a trusted part of security solutions" for 70 percent of those polled.

Bringing on a trusted third party is another option for organizations looking to close the workforce gap. A 2019 report by Deloitte found that 99 percent of large organizations had outsourced at least some of their cybersecurity operations.

The key to protection is to start with the basics: Establish a strong patch management program, create policies that ensure safe password practices and implement computer access procedures that utilize multifactor authentication. All organizations should have a standard external firewall to protect their networks on the edge, but they also may benefit from internal firewalls and segmentation to prevent attackers from moving laterally if they do gain access to their systems.

Detect

Organizations should have solutions in place to enable "timely discovery of cybersecurity events," according to NIST. These tools should be designed to:

- Ensure that anomalies and security events can be detected and understood
- Include continuous monitoring capabilities to track cybersecurity events "and verify the effectiveness of protective measures, including network and physical activities"

Respond

In the event of a data breach, organizations should have a detailed plan in place for responding to the incident as quickly as possible. According to NIST, that response should include, among other things:

- Mitigation activities performed to contain and resolve the breach
- Forensic analysis to determine the impact of the incident
- A plan for incorporating "lessons learned from current and previous detection/response events"

Recover

The last of the NIST framework functions is focused on the capability an organization has to restore any services that may be impaired due to a cybersecurity incident. The plan, according to the institute, should "support timely recovery to normal operations" so the impact of any incident is minimized as much as possible.

In the end, creating a strong data security plan requires the organization to be proactive. By establishing policies and procedures and implementing solutions designed to deter and contain attacks, organizations can stay a step ahead of cybercriminals and avoid turning to measures that may prove ineffective.

Data Security Solutions and Services

The good news for any organization intent on shoring up its data security posture is that a variety of solutions and services are available in this arena. Many vendors now believe in taking a layered approach to cybersecurity and offer products that protect the network as a whole while also providing security around individual parts. A trusted partner can help an organization take cybersecurity to an even higher level, providing in-depth consultation services to align security initiatives with critical business objectives.

Here is a look at a few of the solutions and services most organizations should have on their radar as they consider their cybersecurity options.

Cybersecurity Solutions

Next-generation endpoint security: Traditional endpoint protections such as firewalls and anti-virus software were designed to detect and thwart known cyberthreats. Today, however, attackers are more sophisticated, and data protection tools focused on previously identified threats are too reactive to be effective in preventing unauthorized network access. Next-generation endpoint security solutions, which employ AI and machine learning, ensure overall system protection by identifying and eliminating potential threats at every endpoint on a network.

$8.19 MILLION

The average total cost of a data breach in the U.S. in 2019[2]

Next-generation firewalls: Much like traditional firewalls, next-generation firewalls provide stateful inspection of an organization's network traffic, but that's where the similarities end. Gartner describes next-generation firewalls as "deep-packet inspection firewalls that move beyond port/protocol inspection" to include intrusion prevention and application visibility. Most important, next-generation firewalls use threat intelligence from the cloud to identify and adapt to evolving security threats.

Email security: While strong passwords and employee vigilance are indispensable when it comes to email security, automated tools that protect against viruses and malware are critical as well. The best solutions offer organizations comprehensive protection of their email infrastructure by intercepting threats before they can spread.

Cloud security: Cloud security technologies are designed to protect data stored or transmitted beyond the network perimeter. A typical cloud service might provide security solutions that include identity and access management tools (encryption keys, for example), infrastructure protection, threat detection and continuous monitoring, and dedicated data protection tools such as hardware-based key storage for regulatory compliance.

Cloud access security brokers: CASB solutions enforce security policies for users and systems that access cloud-based services via user authentication, device profiling, malware detection and other protective measures.

Software as a Service: SaaS solutions are delivered by a cloud provider on demand. One key advantage associated with SaaS has to do with its versatility: Users can access SaaS applications anywhere there's an internet connection. And because the software is in the cloud, the vendor can apply critical patches and updates instead of relying on users to do the job themselves.

Data loss prevention: Data loss prevention tools and processes are designed to prevent valuable data from being misplaced or misused. Built around an organization's particular security policies, DLP solutions automatically identify any violations and then enforce protective measures to ensure data safety.

Identity and access management: IAM solutions give organizations a secure and centralized way to manage user identities and access permissions. Through identification and authentication processes (such as passwords, biometrics and tokens), IAM ensures that those who are authorized have the network access they need, while those who are not authorized to have access are kept out.

Cybersecurity Assessments

A third-party cybersecurity assessment can help an organization understand its current security posture and identify the threats facing its data. A variety of such services are available and appropriate, depending on the specific needs of an organization:

Data Protection with a Zero-Trust Architecture

The "zero-trust" model of cybersecurity is based on the premise that an organization should never trust an entity inside or outside of its network perimeter until the entity's identity and authorization is verified. This "everyone is guilty until proven otherwise" approach has gained acceptance as a best practice in recent years as a means of controlling the damage attackers might do in the event they gain access to an organization's systems. A zero-trust security architecture relies on five primary network controls to ensure data protection:

1. Segmentation: Dividing an organization's network into multiple secure segments keeps traffic to areas where it is permitted. This tactic can prevent an attacker from causing widespread damage by limiting his or her ability to roam the network.

2. Identity and access management: IAM allows an organization to confirm user identities through approaches such as multifactor authentication. It also ensures that once users have access to the network, they stay within the scope of their authority.

3. Least privilege: The principle of least privilege holds that any entity that requests access to a network or segment should be assigned only the minimum rights and privileges needed to achieve that entity's business goals.

4. Application inspection: A firewall equipped with application inspection technology ensures that both inbound and outbound network traffic are safe and coming from legitimate sources.

5. Security event analysis: With a security information and event management (SIEM) tool, IT professionals can access network log, alert and event data for a holistic view of their security posture and insight into changes they can make to improve.

Source: [2]IBM, "2019 Cost of a Data Breach Report," July 2019

Vulnerability assessment: This involves an automated evaluation of current IT systems to root out potential weaknesses. Regular vulnerability assessments can help organizations stay on top of evolving threats by classifying and ranking vulnerabilities in order of priority.

Penetration testing and application assessment: This includes manual "ethical hacking" to identify vulnerabilities such as ineffective passwords and issues with software and hardware that may present risks to an organization.

Configuration review: Here, systems are tested to ensure they're configured in accordance with accepted best practices. Results can be used to recommend improvements.

Social engineering: Custom phishing scams and other simulated attacks are deployed to test an organization's preparedness for dealing with the real thing.

Framework assessment: This involves an evaluation of an organization's current security posture as compared to the end state of a cybersecurity framework. By conducting a gap analysis of an organization's current state and its target state, a partner can lay out the steps needed to get the organization into a more effective posture.

Compliance assessment: Here, the identification of compliance-related data security issues helps an organization meet regulatory requirements.

CDW: We Get Data Security

As cyberthreats evolve and become increasingly sophisticated, experts can help you optimize your organization's data security strategy. At CDW, we understand the importance and intricacies of IT compliance, and we also know that it's just the first step toward a comprehensive cybersecurity plan.

As a provider of data protection tools and services for business organizations, government agencies and educational institutions, CDW is a proven leader in the world of cybersecurity. We provide organizations with the people, the products and the plans they need to build in-depth cybersecurity solutions that can stand the test of time. Among the specific IT consulting services and solutions we offer to help determine your security needs and remediate active threats:

- **CDW Threat Check:** A complimentary vulnerability assessment to monitor malware and other security threats and identify infected devices and compromised connections
- **Comprehensive Security Assessment:** An engagement to manually uncover vulnerabilities using the same hacking strategies as cybercriminals (penetration testing)
- **Managed Services:** An engagement in which trained experts serve as an extension of your IT team using a cloud-based security information and event management (SIEM) solution to monitor and respond to threats and help with logging compliance requirements

Ensuring data security at every level of an enterprise is possible only when the stakeholders involved understand their organization's vulnerabilities and goals. It requires a willingness to see your security program as a journey and a process — not something that can be purchased in a box. At CDW, data protection is our business, and we're ready to help at whatever stage of the journey you're on.

CDW AMPLIFIED™ Services

CDW Amplified™ Security services are composed of both information security and network security practices, offer an objective look at your current security posture and provide continuous defense against, detection of and response to growing threats.

DESIGN for the Future
All CDW Amplified™ Security services provide a comprehensive approach to prevent data breaches and proactively respond to cyberattacks.

ORCHESTRATE Progress
CDW Amplified™ Security engineers can assist with installation and deployment of advanced security techniques and ensure technologies are optimized for your needs.

MANAGE Operations
We can manage security solutions for you, helping you stay vigilant and maintain compliance while easing the burden on your IT staff.

Sponsors

TREND MICRO paloalto NETWORKS FORTINET SOPHOS

Want to learn more about how CDW can help you improve your data security? Visit CDW.com/security.

CDW PEOPLE WHO GET IT®