Volume One / Issue Two

BANK OF AMERICA

Cyber Security Journal

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

INSIGHTS ON THE NEXUS BETWEEN PEOPLE, TECHNOLOGY AND BUSINESS

EVERYTHING'S CONNECTED

The challenge of staying safe as the Internet of Things revolutionizes work

RANSOMWARE RAMPS UP

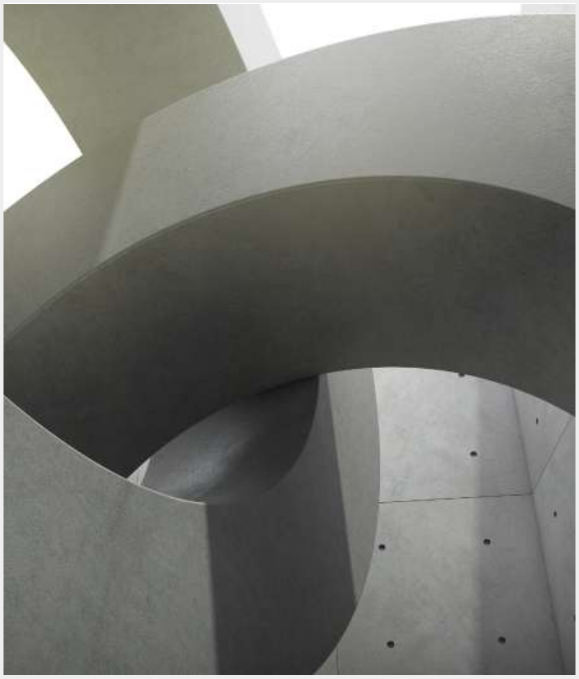
Learn more about a growing threat to business operations and data

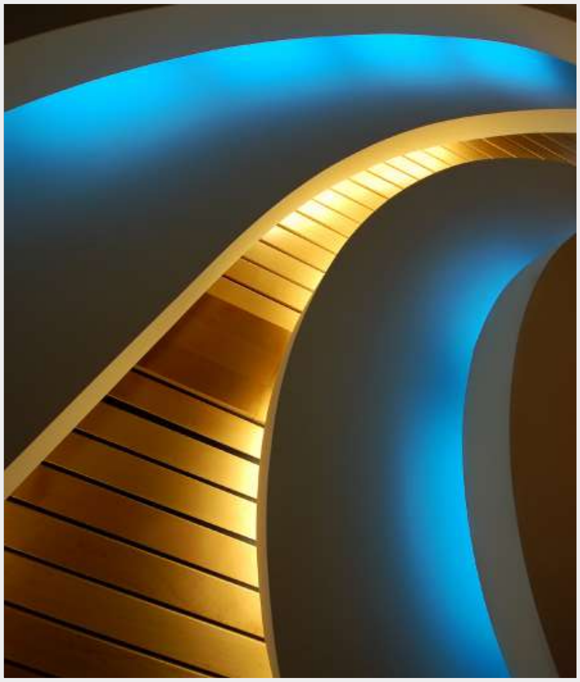
Contents

Cyber Security Journal • Vol. One / Two

Letter

Features





Neither Bank of America nor its affiliates provide information security or information technology (IT) consulting services. This material is provided "as is," with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this material, and without warranty of any kind, express or implied, including, but not limited to, warranties of performance, quality and fitness for a particular purpose. This material should be regarded as general information on information security and IT considerations and is not intended to provide specific information security or IT advice nor is it any substitute for your own independent investigations. If you have questions regarding your particular IT system or information security concerns, please contact your IT or information security advisor.

We're Committed to Helping Protect You

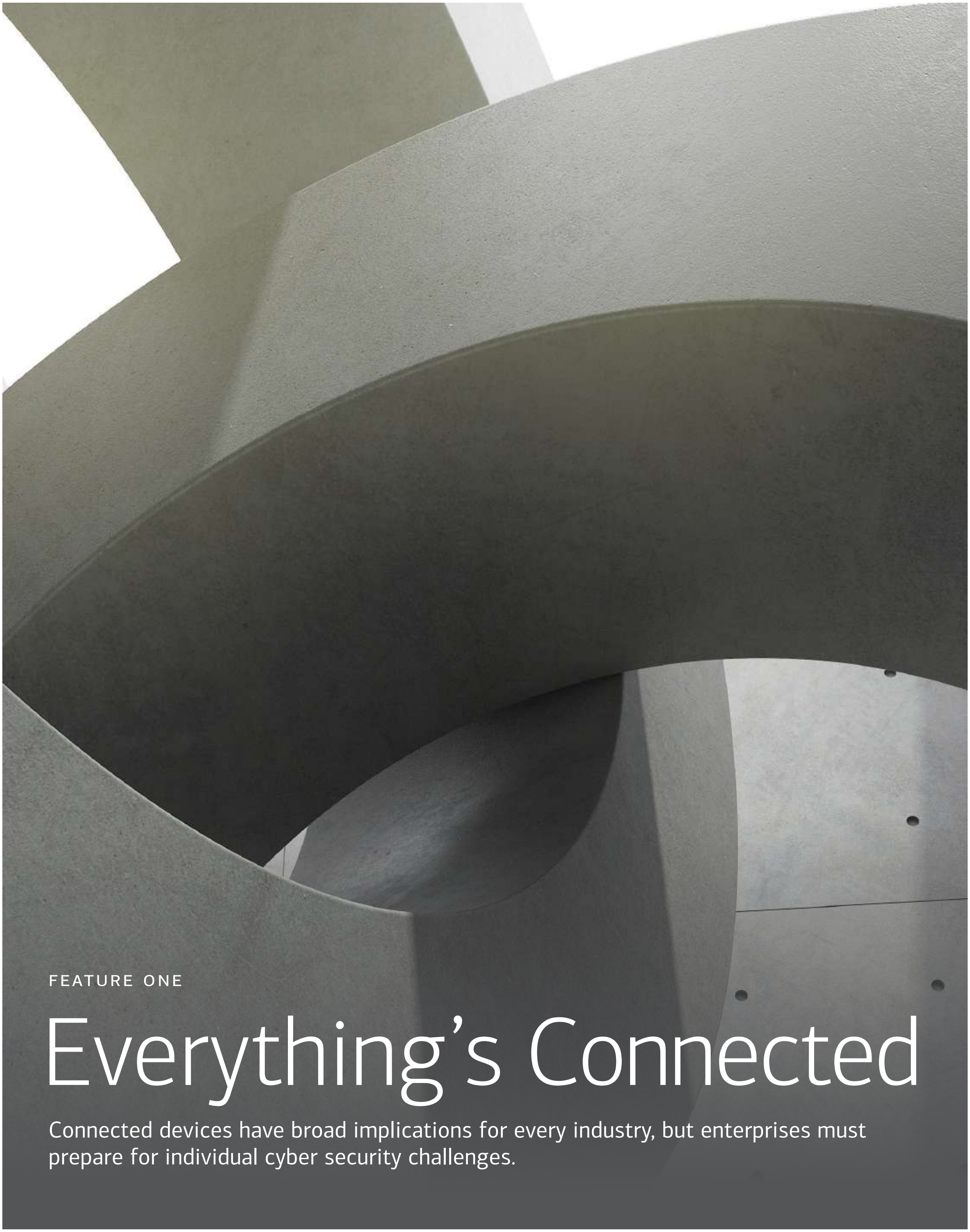
Craig Froelich

Information security is a top priority for Bank of America because the trust of our clients and customers is fundamental to our business. As part of our ongoing commitment to protect you, your business and the communities in which we operate, we are happy to share the second issue of our Cyber Security Journal. This content is intended to deepen your knowledge about the latest cyber threats, while sharing best practices to bolster your defenses.

In this issue, we explore the Internet of Things and Ransomware. During the pandemic, consumers are moving around less and shifting more of their transactions online. The more we connect our lives to the internet, the more vigilant we have to be, because where we go, cyber criminals go. All your devices at home and work are connected to the internet, and you should make sure that they all are secure. A multi-layered information security approach is always your best defense.

Thank you for putting your trust in us.

Chief Information Security Officer, Bank of America



FEATURE ONE

Everything’s Connected

Connected devices have broad implications for every industry, but enterprises must prepare for individual cyber security challenges.

Internet of Things

The Internet of Things drives automation in manufacturing and processing.

The Internet of Things (IoT), the global network of connected or “smart” devices, is driving innovations around operations, manufacturing, maintenance and customer experience. Given the concurrent development of technologies such as 5G and its support of edge computing, IoT’s disruptive potential seems almost limitless.

But without proper security, can businesses harness the full potential of these devices? For many technology experts, the answer is almost certainly no.

Companies have to fully consider the risk-reward ratio of any deployment of connected devices and their networks. But this type of assessment is made increasingly arduous by the sheer number of connection points. It’s predicted that a total of 41.6 billion devices will be connected to the internet by 2025, generating an astounding 79.4 zettabytes (ZB) of data that year.[1]

For businesses, the use cases of IoT devices are virtually boundless. They can help streamline supply chains, facilitate production and manufacturing processes, remotely monitor and maintain equipment and provide real-time monitoring of logistics and assets in transit, to name a few.

Yet while connected devices allow organizations to automate a plethora of activities, they also introduce risks. That’s because every device connected to the internet expands an organization’s cyber landscape and becomes yet another potential source of cyber compromise.

It’s not surprising, then, that IoT-related cyber incidents are mounting. More than one in

Defining IoT and IoT devices

The Internet of Things (IoT) is a network of connected physical objects that contain embedded technology to communicate information among other devices using the cloud.

IoT devices are typically simple devices or sensors that wirelessly connect to a network and perform limited functions. They often have limited memory and compute capabilities.

four (26%) respondents to a study on third-party IoT risk say their organization experienced a data breach due to unsecured IoT devices or applications in 2019, compared with 15% in 2017.[2] Perhaps more worrisome, another study found that 74% of enterprise security professionals believe their security controls and practices are inadequate for unmanaged and IoT devices.[3]

Traditional connected devices are subject to typical cyber security risks, such as theft of sensitive data and exposure to malware. But because their supporting platform combines the digital and physical worlds, IoT risks extend to more damaging compromises of systems and networks that can jeopardize business operations.

Once compromised, an IoT device could launch a distributed denial of service (DDoS) campaign that uses internet traffic to disrupt systems and operations. An array of compromised devices could exfiltrate user credentials or bank account information. Cyber criminals can infiltrate operational technology (OT) to remotely control a manufacturer's assembly lines or disrupt national security by shutting down power grids.

Connected remote and edge devices require new approaches to cyber security.

IoT benefits and risks during a global event

The coronavirus crisis presents a use case for IoT functionality and its concurrent potential risks. Businesses and governments are developing innovative connected apps and technologies designed to monitor, track and mitigate transmission of the disease.

> “Each connected object creates a new endpoint. Since the IoT is a network of connected devices, a single compromised object can potentially disrupt enterprise networks or systems.”

In one example, an owner of an office building in New York installed connected, thermal infrared cameras to measure employees' body temperatures as they enter[4] and also invested in developing a mobile app to monitor compliance with social-distancing rules using smartphone data.

Other IoT devices that are being used to slow the spread of coronavirus include connected thermometers, remote healthcare monitoring, contact-tracing apps and robots that sanitize medical facilities and warehouses.

But given the urgent need, it seems likely that these devices will be rushed to market. Companies eager to adopt these technologies may increase their risk exposure through inadequate assessment of device security features.

How IoT and connectivity intersect

Enhanced performance is also coming to wireless connectivity, a foundational component of IoT infrastructure. The 5G cellular network, when fully deployed, will offer superchargers to throughput with speeds that start at 1 gigabit per second (Gbps).[5] As 5G takes off, forward-thinking businesses are beginning to consider the use of edge computing for IoT security. This distributed topology brings computing and memory functionalities closer to the IoT end device, which can accelerate processing and eliminate delays in transmitting data to the cloud.

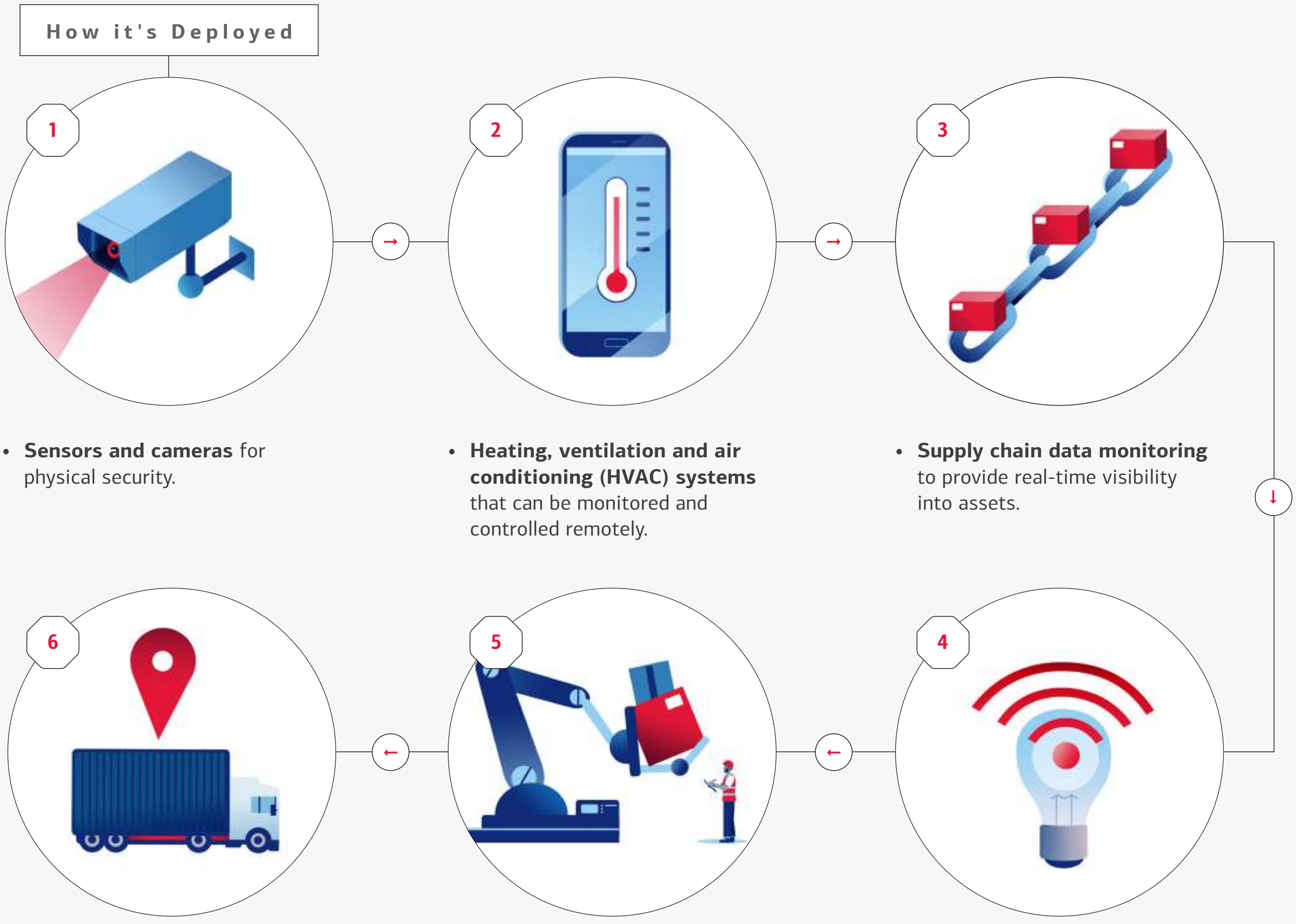
However, securely implementing and integrating these new technologies will require IoT expertise and resources that many companies lack. That's why businesses are turning to device-enablement platforms. These third-party services help companies design, implement and manage IoT platforms. They connect devices, cloud providers and applications on a unified platform, as well as integrate security solutions like endpoint protection, access management and analytics.

IoT security considerations

As IoT vulnerabilities expand across a sprawling ecosystem of connected devices, cyber security becomes increasingly complex and

Connected Device Implementations

IoT technology is changing the way many industries operate, manufacture goods and analyze productivity.



How it's Deployed

1

- **Sensors and cameras** for physical security.

2

- **Heating, ventilation and air conditioning (HVAC) systems** that can be monitored and controlled remotely.

3

- **Supply chain data monitoring** to provide real-time visibility into assets.

4

- **Facilities management tasks** such as predictive maintenance of equipment, intelligent lighting and asset tracking.

5

- **Automated warehouses, assembly lines and robotics** for better inventory control and productivity.

6

- **Logistics and fleet management** that track locations of trucks, equipment and personnel.

Questions to ask when purchasing IoT devices

Five questions to assess and avoid security problems in connected devices.

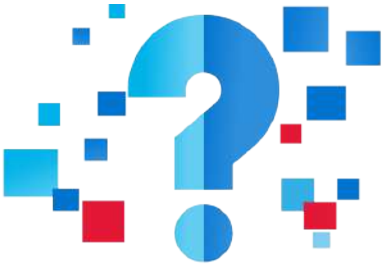
1 **Can its firmware or OS be updated?**
Firmware is permanent device software. With more complex devices, firmware updates may be necessary to keep devices secure.

2 **Will the manufacturer support and provide security updates?**
Some devices are programmed to check for and download updates. Others require users to check with manufacturers.

3 **What level of authentication can the device accommodate?**
Depending on the device's connections or generated data, single sign-on, two-factor authentication or more advanced protocols may be needed.

4 **What level of encryption is available?**
Some devices require extra layers of encryption, which converts data into code that is difficult to break.

5 **Can the device be remotely controlled and monitored?**
IoT monitoring may allow users to access device data, gauge its performance and evaluate its security status.



Connected remote and edge devices require new approaches to cyber security.

difficult to scale. That's because businesses must understand a plethora of different devices and their unique security risks, as well as protect their growing data footprint.

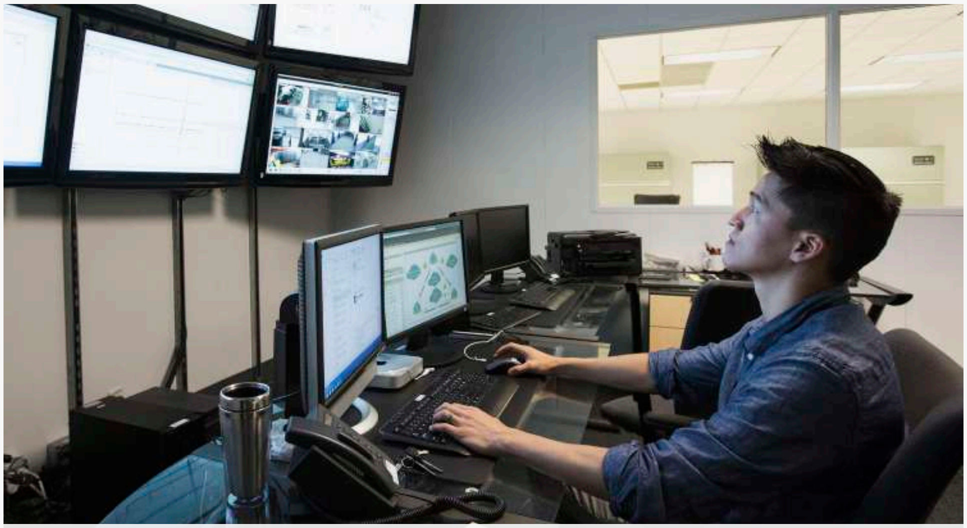
Each IoT object creates a new endpoint of a network, and since the IoT is a network of connected devices, a single compromised object can potentially disrupt enterprise networks or systems. Compounding matters, IoT systems and devices are often not properly managed — or not managed at all — and businesses often don't have IoT-specific security controls. Also lacking is an adequate grasp of IoT risks: One study of IT professionals found that 51% don't fully understand the risks associated with IoT devices.[6]

When developing an IoT security program, the first step is to identify, classify and locate all IoT devices connected to the enterprise network. As more devices are added to the network, and the threat landscape evolves, regular reassessments of this nature are critical. Yet at this stage of IoT adoption, these best practices are far from universal: In fact, 41% of technology decision-makers say they lack visibility into their unmanaged and IoT devices.[7]

Businesses also need to ensure that devices can be configured to meet their specific needs and that their embedded firmware or operating system (OS) can be updated with patches. It's also important to be able to segment devices on enterprise networks, either as an individual virtual land area network (VLAN) or virtual router instance.

“Third-party services are helping companies design, implement and manage IoT platforms. They connect devices, cloud providers and applications and integrate security solutions."

Locking down the device's communications capabilities is critical to data protection and network security. Following the principle of least privilege, which limits access privileges for users and pro-



Cloud providers can help businesses secure their IoT devices and networks.

grams to the minimum needed to perform their tasks, organizations should implement controls that allow an IoT device to communicate only with the entities necessary to perform its stated function.

Most IoT implementations connect to the cloud to send and receive data, and both the devices and the cloud service should be able to perform mutual authentication. But there is little standardization among IoT devices, and that complicates integration and hinders scalability. Major cloud providers address these needs by offering platforms that help businesses securely implement IoT platforms, as well as integrate data management and analytics, device integration, network monitoring and cyber security capabilities.

And because cyber criminals can gain access to a company's IT systems via compromise of a business partner's systems, devices and software, it's critical to assess security capabilities of third parties based on the principle of least privilege. Then, limit the systems and devices with which vendor IoT devices can communicate.

A new approach to cyber security?

IoT adoption is all but inevitable for many businesses. To stay competitive and innovative, many will feel compelled to follow where the technology leads.

However, smart companies can limit their risk even as device security is in catch-up mode. Understanding how IoT devices and networks change the thinking around cyber defenses can aid risk assessment and improve business outcomes, whether a company is pursuing an aggressive or gradual adoption strategy. ■

IoT

Key takeaways:

- Organizations should be able to identify, classify and locate every IoT device connected to their network.
- Network segmentation and access management can limit the systems and devices with which vendor IoT devices can communicate, which can diminish the attack perimeter.
- IT staff must help the enterprise to raise overall awareness of IoT security concerns and controls.

[1] IDC, "The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast," June 18, 2019.

[2] Ponemon Institute, "The Third Annual Study on Third Party IoT Risk: Companies Don't Know What They Don't Know," May 2019.

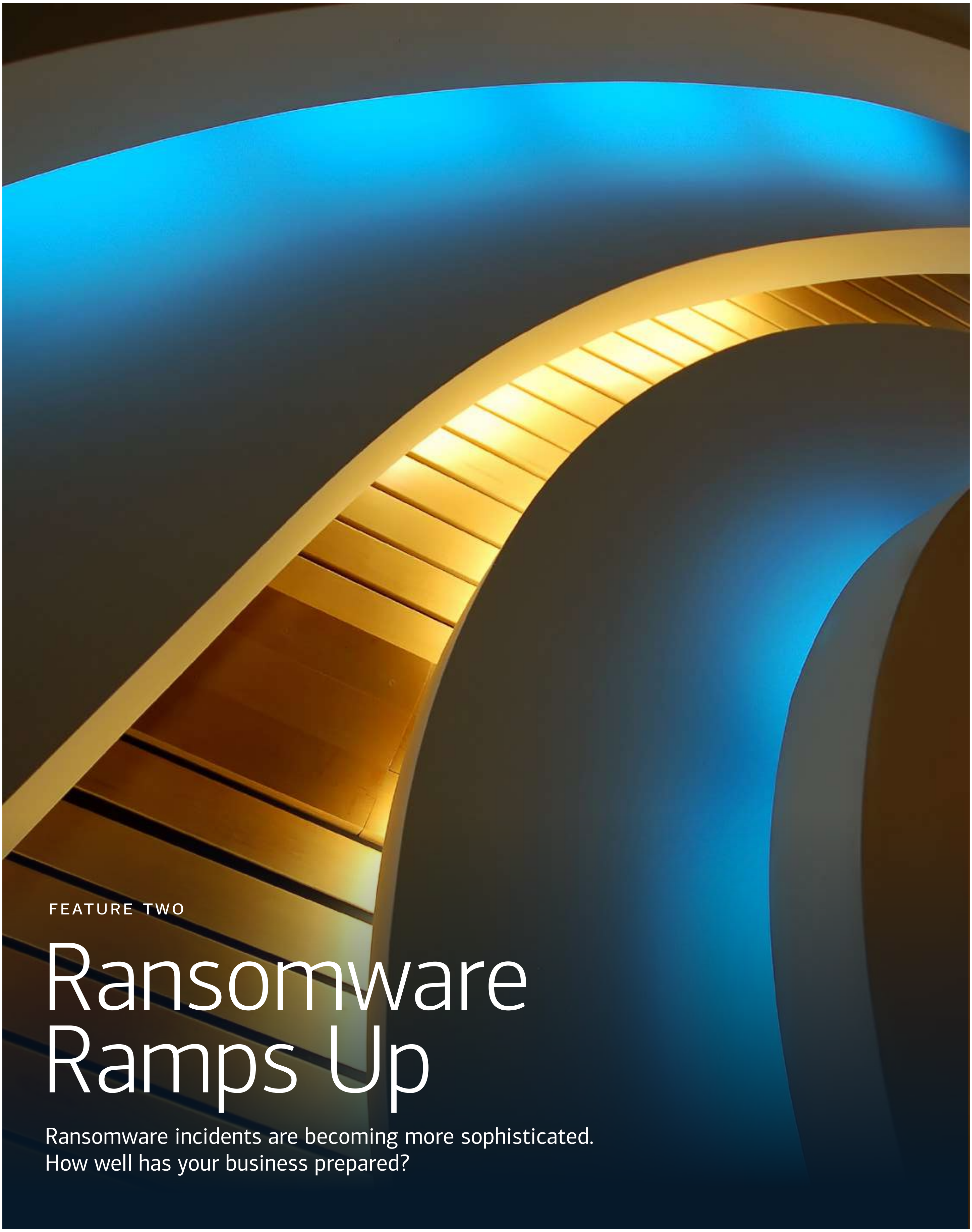
[3] Forrester Research, "State of Enterprise IoT Security in North America: Unmanaged and Unsecured," September 2019.

[4] The Wall Street Journal, "Welcome Back to the Office. Your Every Move Will Be Watched," May 5, 2020.

[5] Deloitte, "Private 5G networks: Enterprise untethered," Dec. 9, 2019.

[6] Forrester, "State of Enterprise IoT Security in North America: Unmanaged and Unsecured," September 2019.

[7] Ibid.



FEATURE TWO

Ransomware Ramps Up

Ransomware incidents are becoming more sophisticated. How well has your business prepared?

Ransomware

Ransomware attempts may seek to capture data or disrupt a company's operations.

In 1989, epidemiologists at a World Health Organization conference found themselves recipients of a nonbiological agent that would eventually become a different type of global scourge than the ones they were studying. A biologist at the conference handed out 20,000 floppy disks to researchers from 90 countries. Supposedly containing a questionnaire on disease research, the disks carried a crude form of malware demanding each victim send $189 to a post office box in Panama. The perpetrator was eventually caught, and ransomware had been born.

Today, ransomware is delivered through links and attachments in increasingly varied ways: fake emails, sham websites spoofed to look official, poorly secured remote access services or pop-up warnings with phony links for technical support. Clicking those links or attachments loads software onto the system, which then downloads ransomware that invades the network and encrypts files, rendering a company’s data inaccessible. A ransom note arrives, threatening to destroy data if demands for anonymous payment — usually in the form of an untraceable cryptocurrency such as Bitcoin — are not met.

The deployment of ransomware has skyrocketed in recent months. In 2019, 205,280 organizations confirmed they had files that had been hijacked in ransomware incidents — a 41% increase over the year before, according to IT security firm Emsisoft. The average payment to release hijacked files spiked to $84,116 in the last quarter of 2019, more than double the average payment in the quarter before. In the final month of 2019, that average doubled again to $190,946. Several organizations have faced ransom demands in the millions of dollars.

Ransomware is so lucrative that organized cyber crime syndicates now build prepackaged ransomware kits and sell them on the dark web, allowing criminals with rudimentary technological knowledge to launch incidents against unsuspecting businesses.

A paradigm shift

There’s a very simple reason that ransomware is proliferating so fast: It often works, because victims face a ticking clock and severe impacts on business operations. For businesses of all sizes, the integrity of and access to data is crucial to operations, and many fear the negative impacts on brand and reputation should a data breach become public.

Any business communication channel is a potential ransomware vector.

Additionally, ransomware has become more potent. Earlier variants used encryption that had its own vulnerabilities, but the potential payoff has driven innovation among a more professional class of cyber criminals.

In early stages of the threat, rudimentary ransomware encrypting was exploitable or reversible. But there's been a paradigm shift in recent years, in which major cyber criminal groups have gone to great lengths to implement proper encryption.

If a network is infected with ransomware that implements encryption effectively, the only way to recover data is by using keys held by the ransomware operators. Knowing that there is potentially no tool for recovering data further incentivizes victims to pay.

What's a business to do?

Even when ransomware incidents don't make the news, their impacts can ripple outward. In addition to data loss and reputational damage, there is real potential for intellectual property theft. Depending on the nature of the business, there also may be pressing confidentiality violation issues. If company data is covered by the Health Insurance Portability and Accountability Act, the General Data Protection Regulation, the California Consumer Privacy Act or other laws and regulations, there may be fines and penalties that apply in the event of a breach. In addition, regulations and some contractual obligations require notification of third parties if company data is compromised.

> *“Ransomware is so lucrative that organized cyber crime syndicates now build prepackaged ransomware kits to sell to criminals with no sophisticated technological skills.”*

Avoiding ransomware is complicated by the fact that employees increasingly are bombarded with messaging on devices used in both the workplace and at home. As counterfeit sites and fake emails become more and more convincing, how can businesses prevent employees from inadvertently exposing data as a result of ransomware incidents?

To a large extent, the problem is a product of human error, such as clicking on links in compromised messages. In 2019, phishing was the most common threat vector and was used 90% of the time to gain access to the targeted network. But when employees know what to look for, they are less likely to click on an email or open an attachment or document they shouldn't.

A proper awareness program should provide educational materials and mandatory training that describe in detail the nuances of phishing, a wide-reaching cyber campaign that targets multiple people, and spear phishing, a more direct campaign that seeks information from targeted individuals. Firms should develop a testing program to mimic phishing and a procedure for tracking employees who click and fail the test. Regular tabletop exercises can help employees visualize a ransomware scenario and clearly understand their roles in response and recovery.

Back it up

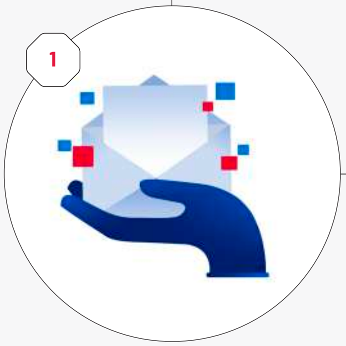
Companies — particularly small and medium-size businesses without the resources to pay large ransoms or those that are unable to endure service interruptions — should employ anti-malware programs to

Continued on page 14

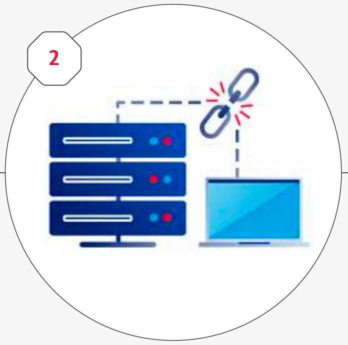
Key Threat Vectors

As new types of ransomware launch, these delivery methods are among the most common.

How it Works



- **Email.** Phishing emails or spoofed communications that appear to come from trusted sources may include links or attachments can contain ransomware.



- **Remote control** provides offsite control of work computers, but cyber criminals can exploit weak remote control credentials to launch ransomware.

- **Pop-ups.** Ransomware can be embedded in pop-up alerts that recommend immediate remedial action and activated when users follow action prompts.

- **Drive-by downloads.** Ransomware can load onto legitimate websites when criminals detect weaknesses in the back-end software.

- **Mobile devices.** Criminals can exploit personal or company-issued devices when employees use public Wi-Fi or applications with poor security features.

- **Vendors and supply chains.** Cyber criminals may launch ransomware from compromised accounts that belong to established vendors or third parties.

Ransomware Preparedness and Recovery Response

Is your organization ready to defend against ransomware attacks and resume operations after an incident? Use this list to enhance readiness

1 **Execute regular backups and testing.** Some ransomware can encrypt local backups as well as primary files. Make sure your system has sufficient layers of defense, including offsite or cloud storage.

2 **Update security software.** Be certain that cyber criminals are doing their homework and looking for new ransomware attack vectors. Regular updates can neutralize many threats.

3 **Regularly monitor operations systems.** Make sure the most current patches and updates are installed.

4 **Update third-party vendor lists.** You are only as cyber-secure as those you do business with. Routinize accounting of established business relationships and assess their access to your networks.

Ransomware Trends

Ransomware names that made the news in 2019:
- WannaCry
- CryptoLocker
- Dharma
- Sodinokibi
- RobbinHood

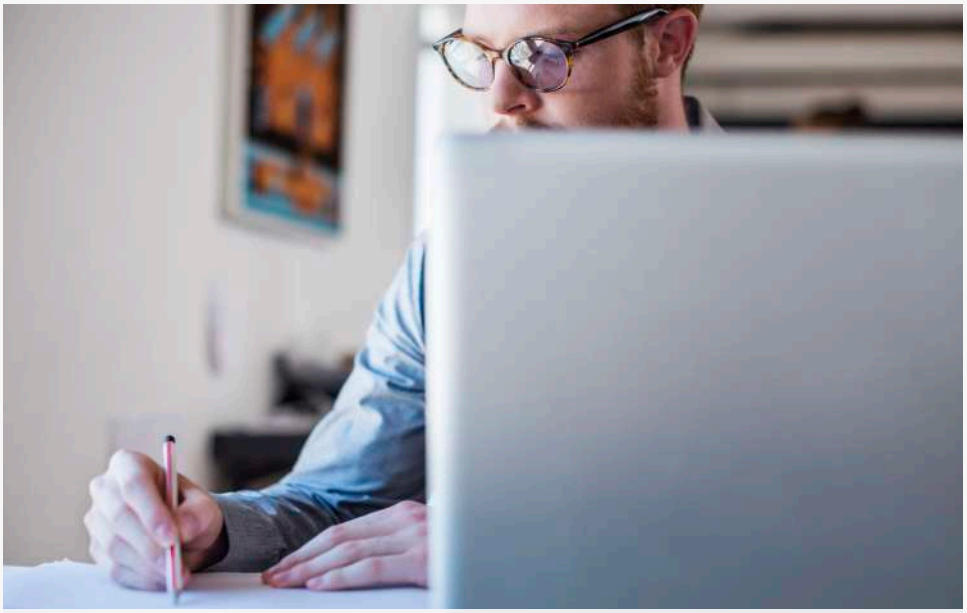
118%
Increase in ransomware attempts in Q1, 2019.[1]

$84,116
Average ransomware payment, Q4 2019.[2]

$111,605
Average ransomware payment, Q1 2020.[3]

1,2 and 3
Rank of public sector, healthcare and public sector as ransomware targets, Q1 2020.[4]

$7.5 Billion
Estimated ransomware damages in 2019.[5]



Cyber criminals may secure access to networks months before they launch ransomware.

Continued from page 12

help monitor their networks for suspicious programs and activities. But even the best technology is only as effective as the people who use it, and because cyber criminals are targeting a broadening array of victims, all businesses should prepare effective, enterprisewide response plans. Some organizations may want to implement wider-ranging resiliency practices that focus on sustaining normal operations during and after a cyber security incident occurs.

Regular and frequent data backups, stored offsite or disconnected from the network, are essential to any recovery plan. Yet many organizations have been slow to take this primary, critical step in a response plan. Companies with backups have options; those that do not have backups, in effect, lack a tenable disaster recovery plan.

> *“Ransomware is a human-error problem. No firm is immune, and education is the most important tool.”*

Vetting the vendors

Businesses also should be prepared to handle disruptions in operation and communication that occur when ransomware makes data inaccessible. Consider the implications of an information blackout that extends across employees’ digital calendars and contact lists. The problems of communication breakdowns can quickly proliferate without an offline communications strategy.

Since so many businesses rely on third-party vendors to execute backups and maintain network security features, it’s critical to evaluate and understand those vendors’ procedures. A key part of ransomware defense is clear com-

[1] *McAfee Labs Threat Report, August 2019.*

[2] *Coveware, “Ransomware Costs Double in Q4 as Ryuk, Sodinokibi Proliferate.”*

[3] *Coveware, “Ransomware Payments Up 33% as Maze, Sodinokibi Proliferate in Q1 2020.”*

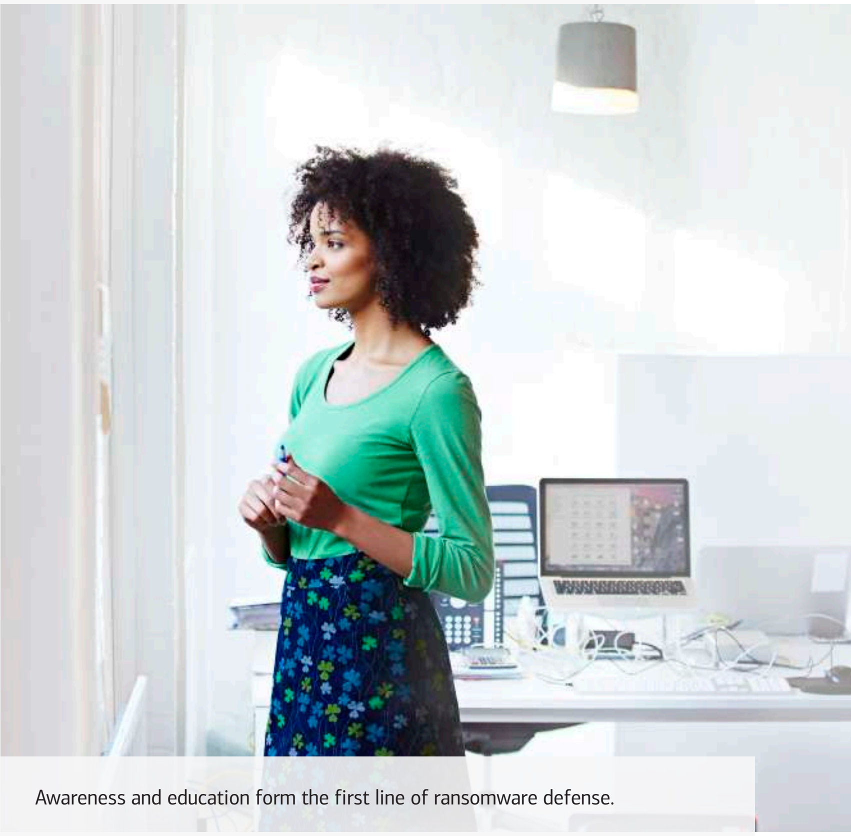
[4] *Ibid.*

[5] *Emsisoft, The State of Ransomware in the US: Report and Statistics 2019.*

> “ *If your network gets infected and you have backups, you have options. If you don’t, you have no options. And that means you don’t have a tenable disaster recovery plan for this type of cyber event.”*

munication with vendors and regular review of their offline communications protocols, their system security tools and strategies, and how they protect confidential information. System and Organization Controls (SOC) reports should cover most of this information, especially if they focus on cyber security risk management.

Still, there have been incidents in which a company trusted an IT vendor who did not have proper controls, which led to the company being compromised. In some cases, the vendor had not taken the basic precautions of changing passwords or implementing two-factor authentication.



Awareness and education form the first line of ransomware defense.

Preparedness mitigates the threat

If a company does experience a ransomware incident, efficient response can minimize the damage. Removing infected devices from the network as quickly as possible may localize the malware, and smart backup protocols can make recovery faster and far less painstaking.

While there is little law enforcement can do to prevent cyber incidents, alerting authorities early can facilitate the collection of evidence, which might help recover funds or data later. Informing all partner organizations, customers and employees of the event also can speed recovery and bolster a company’s reputation for transparency.

Because ransomware provides strong incentives for victims to pay criminals quickly, and law enforcement remains unable to stem the proliferation of cyber incidents, it seems unlikely that ransomware threats will diminish anytime soon.

Ultimately ransomware prevention is a collective practice. Employees and organizations can incentivize one another to share technology implementations and prevention information. Although ransomware tools and methods are increasingly sophisticated, the best defense remains rooted in cyber security basics. ■

Ransomware

Key takeaways:

- Think before you click: Ransomware attacks are increasingly sophisticated.
- Prepare: A company with no backup plan has no response plan.
- Know your vendors: Learn about their security and backup protocols.