A CYBERSECURITY INSIGHT REPORT

One Year after the COVID Shutdowns: Healthcare Facilities Still a Target for Network Outages and Breaches

Healthcare Sector | March 2021

Produced by CyberRisk Alliance for Infoblox

CyberRisk Alliance
Business Intelligence Resources

Infoblox
NEXT LEVEL NETWORKING

CONTENTS

EXECUTIVE SUMMARY

> **Infiltration attacks were on the rise throughout the year, especially in the last quarter—they increased by 50% compared to the previous period, and 2020 was the year with the most infiltration attacks recorded . . . the concern is that this trend will continue.**
>
> — IT director, Latin America

The COVID-19 pandemic brought to the fore serious vulnerabilities in the handling and processing of healthcare data. With employees forced to work from home, healthcare security, compliance and risk executives were in turn required to identify ways to handle and process protected health information (PHI) that was moved off the protected networks within hospitals, clinics, medical centers and offices. Like their counterparts in other industries, healthcare IT professionals needed to identify and engage additional cloud resources that meet multiple state, national and international privacy laws and regulations without overburdening their employees or creating new security vulnerabilities.

This report takes a global view of the healthcare industry's cybersecurity response one year after the pandemic took hold in the United States. Drawing on a respondent pool spanning the United States, Latin America, Europe and the Asia/Pacific region, it examines the types of attacks the healthcare industry faces, the solutions companies are deploying to defend themselves and the spending these require.

Among the report's findings for healthcare worldwide:

- Cloud vulnerabilities and misconfigurations, IoT attacks and attacks to manipulate data/statistics are the top cyberthreats healthcare professionals expect to confront in the next 12 months, each cited by nearly 20% of the total respondents worldwide.
- Data breaches were the top attack vector against cloud networks in the past 12 months, cited by 53% of respondents.
- Network outages in the past 12 months cost more than one-third (34%) of respondents $2 million or more. The Asia/Pacific region was hardest hit, with 42% of respondents reporting that network outages cost between $2 and $5 million—more than double the number of any other region.
- While network outage financial losses tend to be lower than data breach losses, they track closely, demonstrating that losses from normal business interruptions can be as expensive and damaging as data breaches.

Attackers are focusing on the cloud as much as, if not more than, in past years as they look for exploitable access to cloud-based servers and data. Looking back at the past year's cloud vulnerabilities, security teams need to shore up defenses against DoS and DDoS attacks, as well as a weak cloud infrastructure to ensure they will not fall victim to new attacks from bad actors.

Protected health information (PHI)—including individuals' insurance information—looms increasingly large in the pantheon of data at risk, highly prized by cybercriminals, according to law enforcement officials, as a black-market payment mechanism for expensive medical procedures.

Gary Cantrell, the former head of investigations at the Department of Health and Human Services (HHS) Office of the Inspector General, describes PHI files as "a treasure trove of information" about an individual. The files contain a patient's full name, address history, financial information and Social Security number, among other personal data. Credit reporting agency Experian puts the value of a healthcare data record at $1,000 on the dark web, compared to a credit card number's value at $5.

Regulatory penalties for PHI breaches can be significant. The Health Insurance Portability and Accountability Act (HIPAA) sets limits on how such data can be used and what companies subject to the law must do if breached. There are regulations about how quickly HIPAA-related breaches must be reported to authorities, and the HHS can levy significant fines for violations, ranging from $100 for negligence to a maximum of $1.5 million per year for serious violations.

This report probes healthcare companies' data protection experiences and concerns. Among other things, it looks at where in the cloud environment attacks are targeted, as well as where companies need to concentrate defenses to stave off massive fines whether by the U.S. or European Union authorities—or both when jurisdictions overlap. In addition to fines, other breach-related costs include recovery and mitigation expenses, additional network security fees, reputational impact and potential loss of future sales, legal- and public relations–related fees and a plethora of ancillary costs. The direct and indirect costs of breaches potentially can be far more than the cost of fines alone.

Other challenges facing the healthcare industry include "cloud jacking"—which one European security manager said "is likely to emerge as one of the most prominent cybersecurity threats." A North American security manager cited cloud-based malware attacks as his main security concern, including misconfiguration of cloud assets and resources. Ransomware, data corruption, distributed denial of service (DDoS) attacks, phishing and multifactor authentication also were cited frequently as serious concerns.

Worldwide, data breaches cost more than $2 million for almost half (43%) of all healthcare organizations that experienced these attacks while network outages from attacks cost an additional $2 million or more for one-third (34%) of organizations. More than three-quarters (78%) of respondents estimated the costs to prevent breaches and network outages were less than $5 million. Considering many of the direct and indirect impacts from these types of attacks (for example, fines, equipment replacement, victim remediation, loss of reputation and customer losses) and the inability to budget for every possible consequence, the cost of a budgeted and planned prevention strategy justifies the investment.

CYBERSECURITY THREATS/ATTACKS

> **It can be as simple as crafting a link and persuading a user to click it, or it can be something much more sinister.**
>
> **— IT director, U.S.**

PHI is highly prized by attackers because it is highly profitable and provides multiple types of monetizable assets, such as financial data, personal data and data that can be used for ransom attacks. Among the most serious threats that healthcare companies face in protecting this highly sensitive data are the misuse of patient data, unintentional actions by healthcare workers to misuse or make PHI accessible to outsiders and supply chain misuse of PHI (such as a translation or transcription service that sends protected patient data over an insecure connection or as open text rather than encrypted data).

Many times these threats only become apparent after a phishing or a man-in-the-middle attack, malicious network traffic, use of a high-risk or vulnerable operating system or simply due to malware on a system that was introduced by a variety of user errors or a malicious attack.

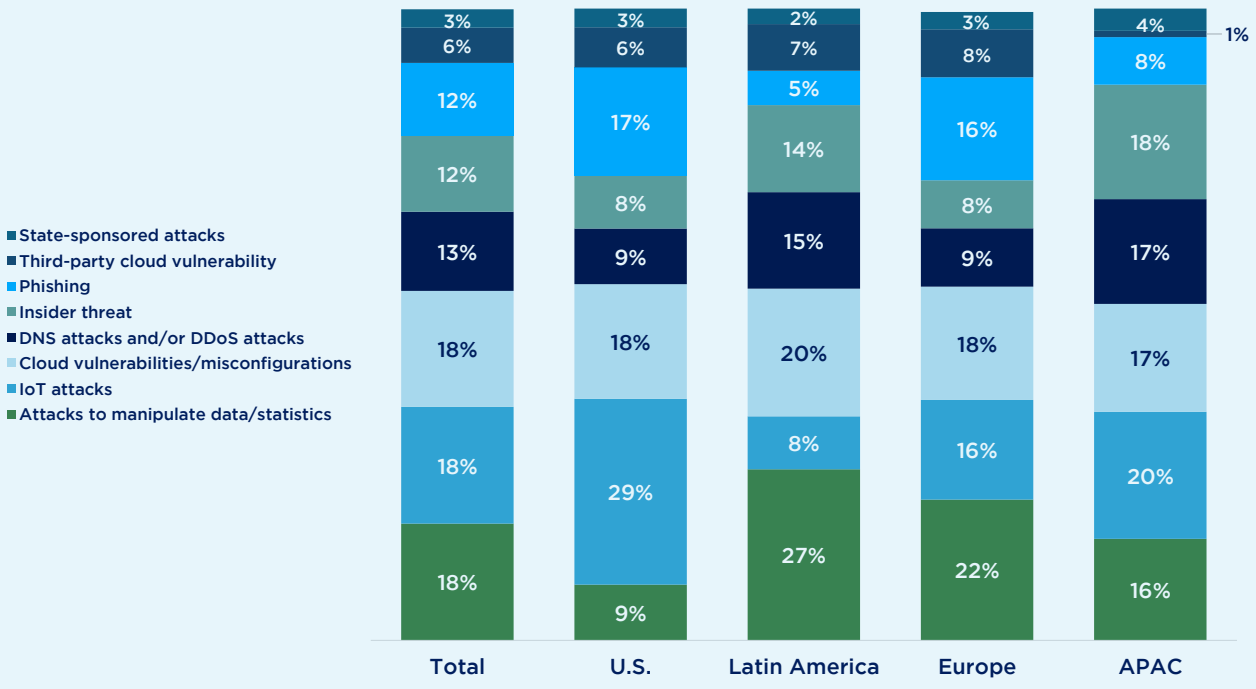
While healthcare data is among the most highly regulated data types, the chart below shows it is not immune to common attack vectors, such as users who click on spear phishing emails, traditional social engineering attacks or carelessness.

Internet of Things (IoT) attacks are among the top cyberthreats, indicated by 18% of all respondents, with the highest incidence in the U.S. (at 29%) and APAC region (20%).

Respondents are also focused on attacks to manipulate data and statistics and cloud vulnerabilities and misconfigurations; they were identified as top threats by 18% of all respondents. This type of attack is designed to harm the reputation and standing of the victim; it is similar to politically motivated

Top IT Security Threats

In your opinion, which of the following is your organization's top IT security threat in the next 12 months?



Note: Percentages may not sum to 100% due to rounding.

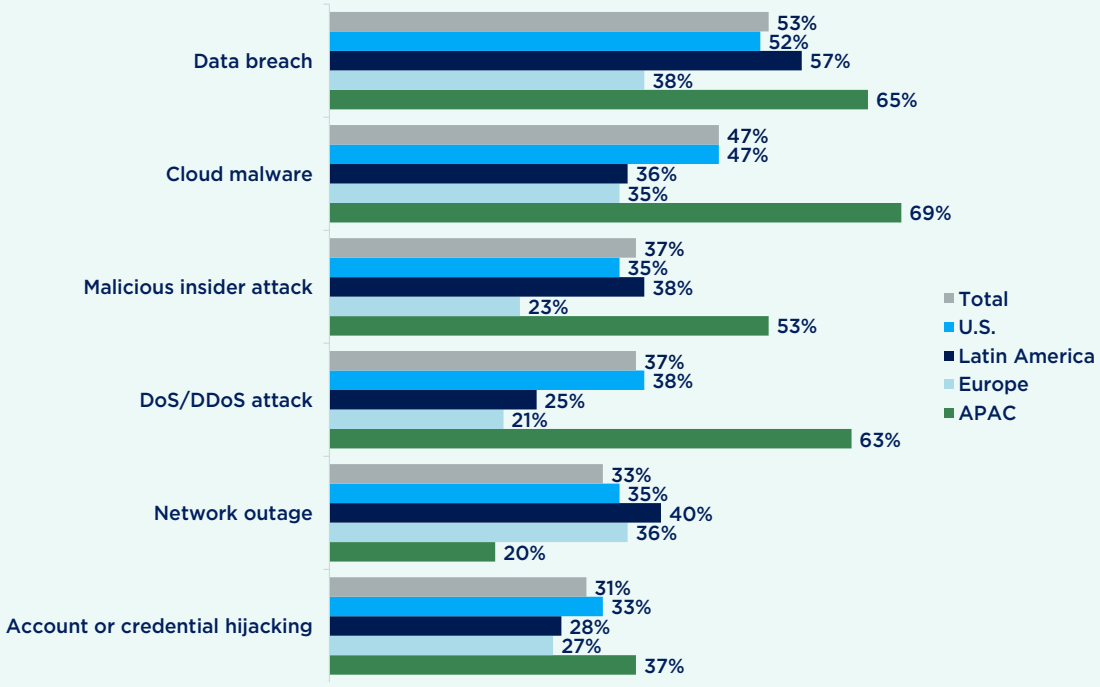
> **We have seen a drastic increase in cyber threats from the past 7 to 8 months. Considering the firm is continuously working toward creating new medicines, we have seen an immense number of malicious activities to steal IP, data and customer information.**
>
> — IT director, U.S.

attacks that show the victim in a negative light. In a healthcare environment, an example would be changing the number of victims of COVID-19 to appear to be much higher than it is, potentially negatively impacting the healthcare provider's reputation and investor confidence. Ultimately, this could be a form of ransomware.

There are, of course, differences between a vulnerability, which might not yet be exploited, and suffering an attack. Over the past 12 months, the majority (52%) of U.S. healthcare industry respondents suffered a data breach, and less than half of U.S. respondents reported other types of attacks against cloud networking assets.

Cloud Networking Attacks

Which of the following types of cloud networking attacks have you experienced in the last 12 months? (Select all that apply)



COSTS AND IMPACTS OF DATA BREACHES AND NETWORK OUTAGES

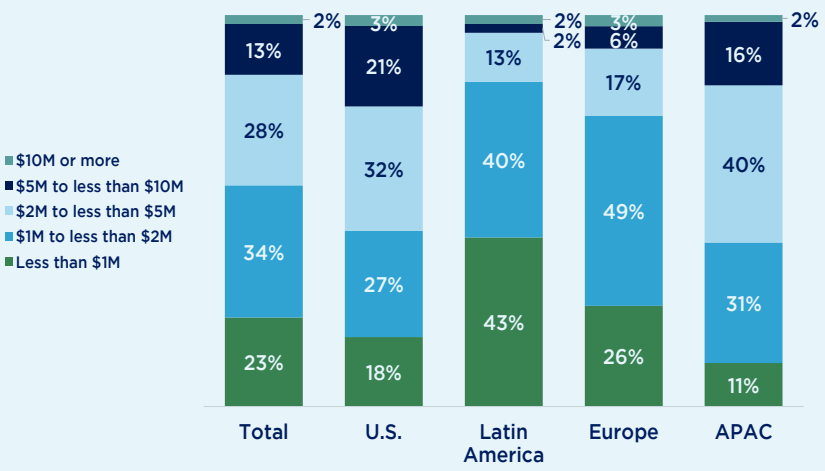
> **The pauses are caused by the attackers, and when there is a connection from the main host to the server, they can steal the handshake—that's when we are vulnerable.**
>
> — IT manager, Latin America

Survey results show Europe has fared best in every category relating to protecting cloud networking assets, perhaps as a result of the European Union's (EU) plans to increase fines for data losses that violate the General Data Protection Regulation (GDPR), which already has some of the highest fines in the world. Recent research by CyberRisk Alliance has also shown Europeans are more proactive in defending against data breaches than their counterparts in North America.

Generally speaking, financial losses for healthcare organizations continue to be high due to data breaches and malware/ransomware attacks. Research shows this industry tends to be among the most popular—and most financially attractive—to attackers. Worldwide, data breaches alone cost more than $2 million for almost half (43%) of all healthcare organizations that

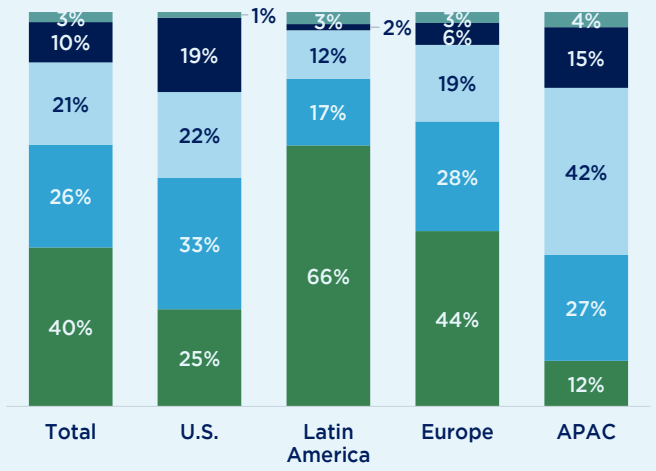
Data Breaches: Financial Losses

What was the average financial loss to your organization as a result of this recent data breach?



Network Outage Attacks: Financial Losses

What was the average financial loss to your organization as a result of this recent network outage?



Note: Percentages may not sum to 100% due to rounding.

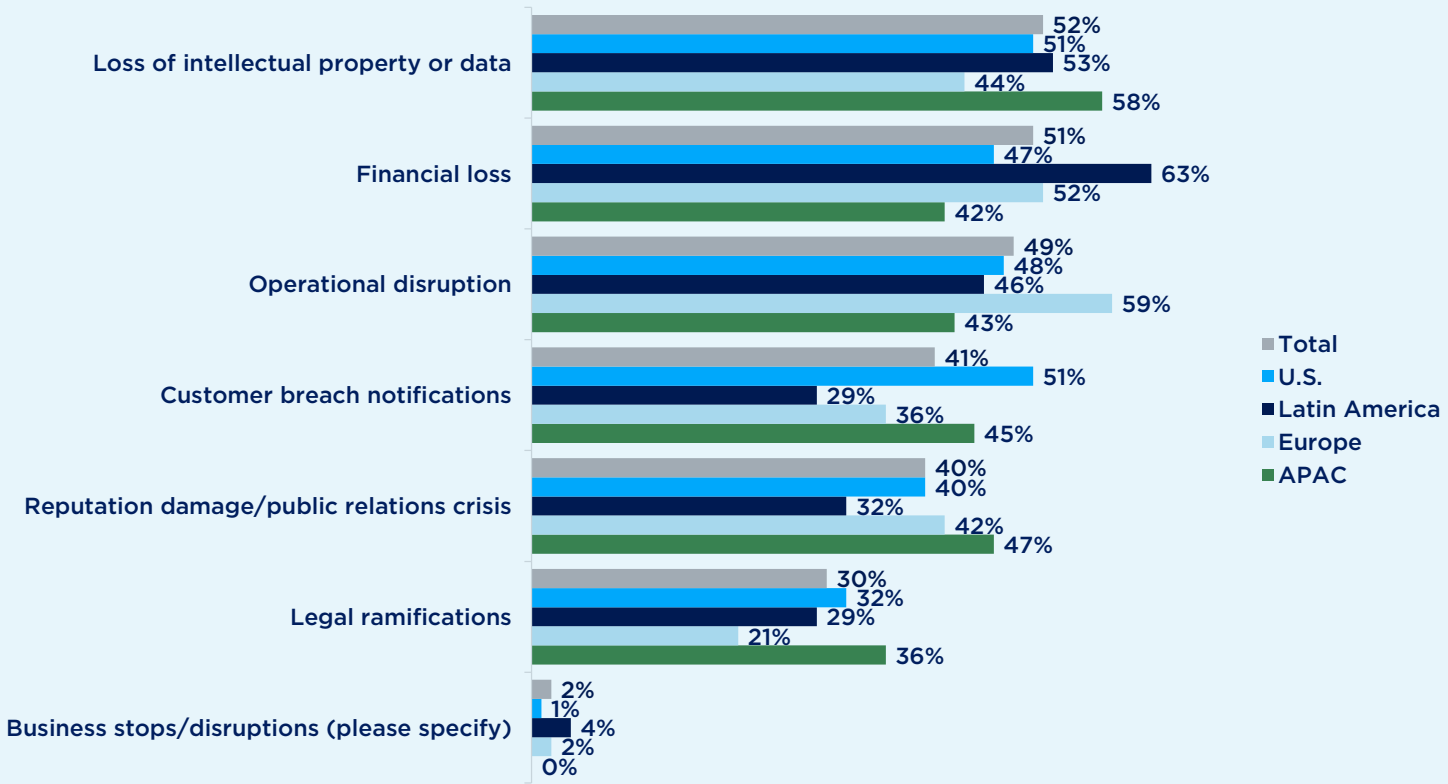
> **The most dangerous—and at the same time most common—attacks such as DoS, and the Domain Name Server, are the most worrying (and effective) if we are talking about the theft of company IDs, that has meant many economic losses.**
>
> — CISO, Latin America

experienced these attacks. Network outages from attacks cost an additional $2 million or more for one-third (34%) of these organizations.

Included in these costs are the remediation and impacts of IP/data losses, financial losses and operational disruptions that were mentioned as the greatest potential consequences of network outages for roughly half of all respondents. Respondents further described concerns about potential business disruptions such as "work stoppages in key areas of data analytics and reporting," "valuable time lost waiting for system recovery," "unplanned resets" and the "loss of clients."

Top Impacts of a Network Outage

What do you think are the greatest potential impacts or consequences to your organization from a network outage? (Select up to 3)



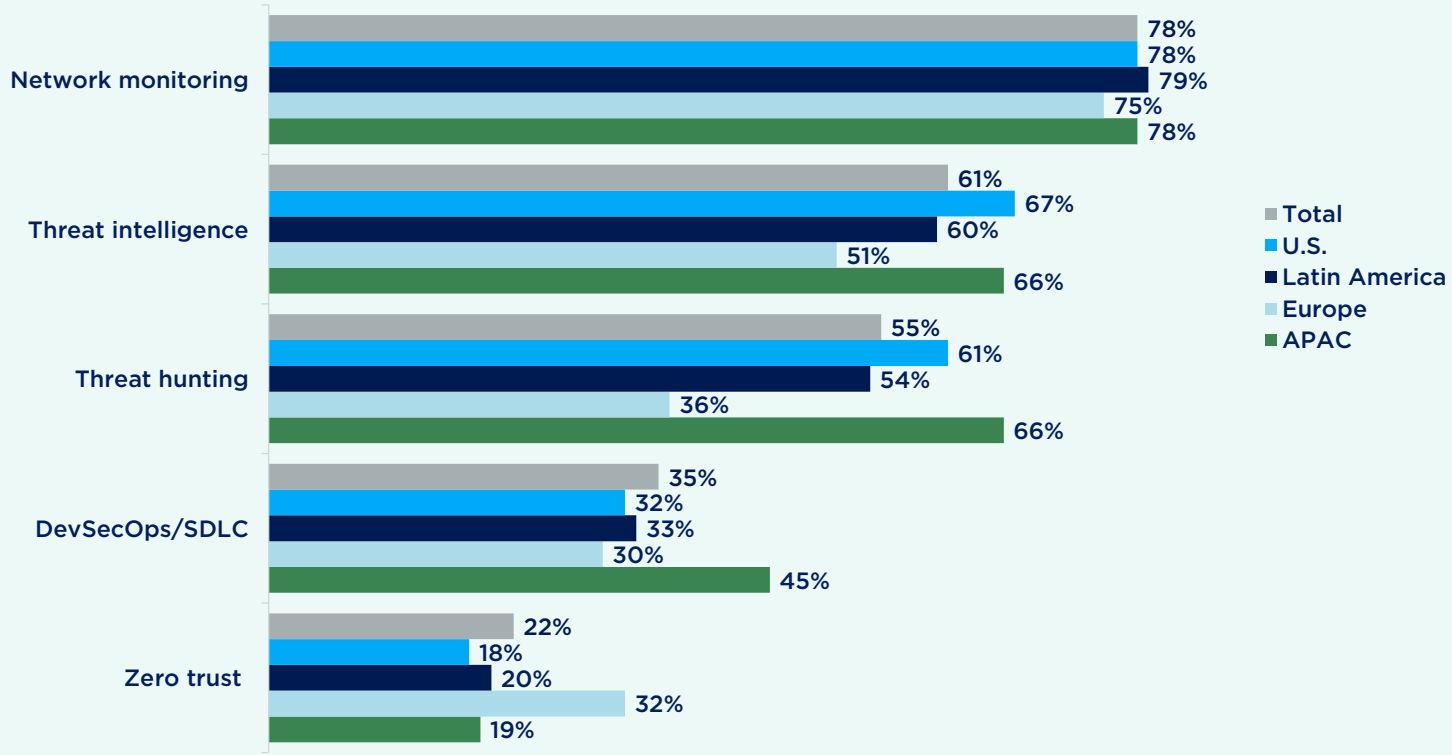
RISK MITIGATION AND SPENDING

> **An increasing number of healthcare providers are using mobile devices at work. Encryption and other protective measures are critical to ensure that any information on these devices is secure.**
>
> —VP of IT, Europe

A major component of the governance, risk and compliance practice is risk mitigation. When healthcare providers learn of possible risks through tools such as threat intelligence and analyzing security information and event management (SIEM) software logs, they can develop courses of action to address those risks in advance. As a proactive security measure, preventing risk is generally more cost effective than remediating risk, which is a reactive strategy. Among the possible tactics in proactively mitigating the risks of attacks or breaches, network monitoring was mentioned by at least three-quarters of all respondents to be the most effective; this was consistent across all regions.

Most Effective Mitigation Tactics

Which of the following have been the most effective in mitigating the risks of IT security attacks or breaches at your organization in 2020? (Select up to 3)



> **Establish a security culture: Ongoing cybersecurity training and education emphasize that every member of the organization is responsible for protecting patient data, creating a culture of security.**
>
> — VP of IT, Latin America

Threat intelligence was also an effective solution for most respondents, with roughly two-thirds of U.S. and APAC respondents reporting this among their most effective methods.

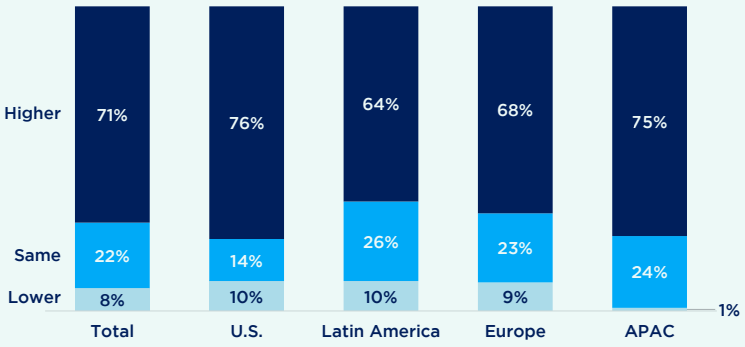
The survey shows 2020 budgets and actual cybersecurity spending increased since 2019 due to the pandemic, and expenditures are expected to be higher in 2021. Across the board those indicating spending decreases are minimal.

A large majority of respondents (78%) estimate the cost to prevent both breaches and network outages to be less than $5 million. This is still less than the financial losses from data breaches, plus the losses from network outages combined with other indirect impacts (e.g., lost reputation, loss of customers and future business and potential fines that are often underestimated); thus the decision to take a proactive security strategy is prudent. Such a proactive mindset, along with an internal culture of security driven by ongoing employee training and management support, is a less costly and more effective approach.

Overall, healthcare organizations are tackling a variety of challenges in protecting their organizations from IT security threats and breaches. Worldwide, more than 40% of respondents indicate they are dealing with educating their workforce, preventing network outages and securing cloud application data. The transition to work from home and the variety of related issues, such as educating employees, increasing IT budgets and monitoring/mitigating risky end-user behaviors are key pain points for the healthcare industry worldwide. Some regions, such as Latin America and Europe, report dealing with these issues at a much higher rate than others.

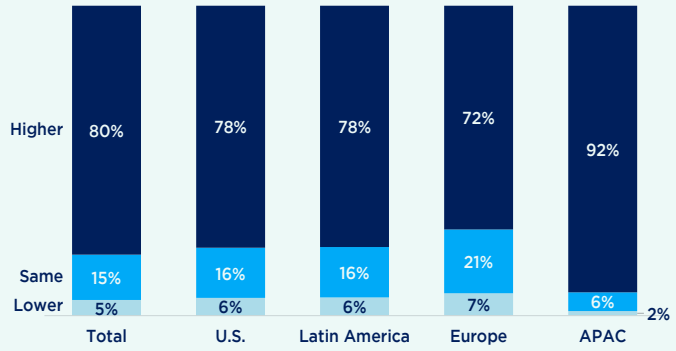
2020 IT Security Budget or Spending Compared to 2019

Compared to our 2019 budget, our total 2020 IT security budget/spending is:



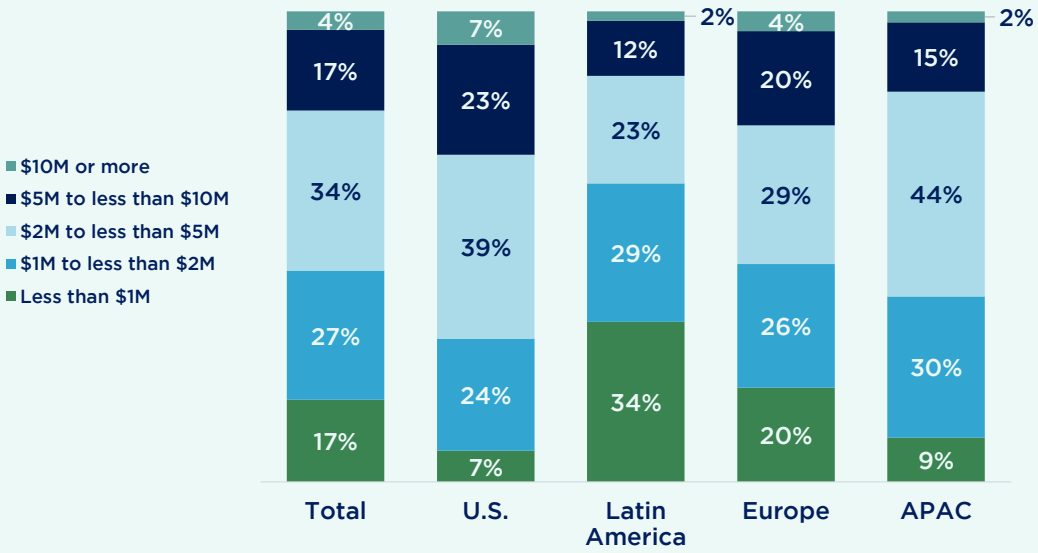
Change in IT Security Budget or Spending in 2021

Compared to our current 2020 budget, our estimated budget for next year (2021) will be:



Projected Costs for Preventing Breaches and Network Outages

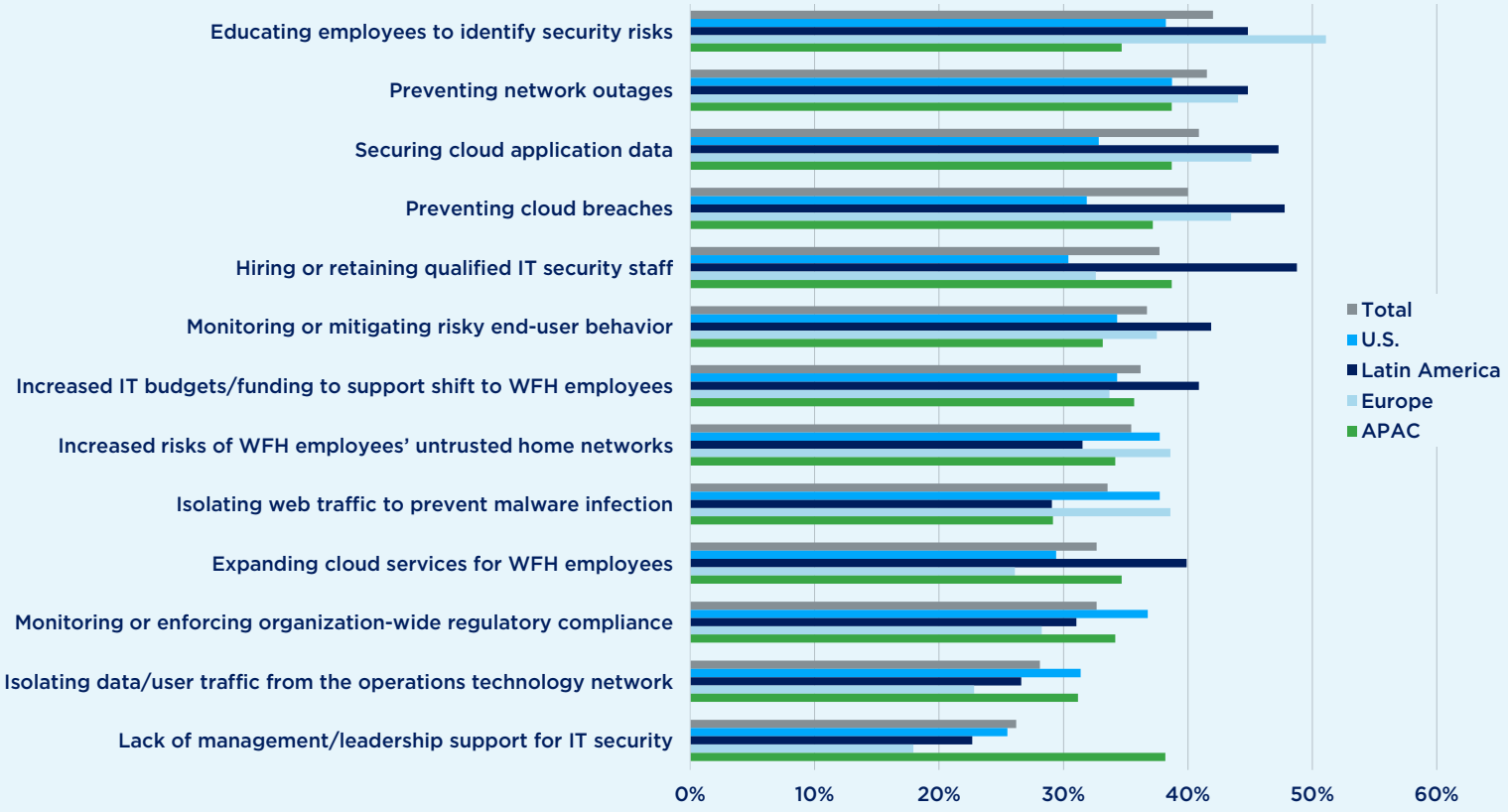
What do you estimate will be your organization's average costs over the next 12 months for the prevention of breaches and network outages?



Note: Percentages may not sum to 100% due to rounding.

Cybersecurity Challenges

What are the top challenges your department faces in protecting your organization from IT security threats and breaches? (Select all that apply)



SOLUTIONS

The FBI reports that there were 59 such attacks on healthcare facilities during the first 10 months of 2020.

Getting a grip on all of the challenges healthcare workers and their management face, especially for remote workers, is indeed vexing. The American Medical Association produced a comprehensive guide, Work from Home During COVID-19 Pandemic, to assist those who desire a more prescriptive approach to security. Aside from detailing what employees need to know about protecting their computing resources, and thus the potential patient data on those resources, it also includes multiple links to recommendations from other agencies.

HIPAA requires covered entities to ensure that patient information is secure, accessible only by authorized persons and used only for authorized purposes. That seems straightforward enough but actually it can be a major challenge. For example, who are authorized users? Is your supply chain safe?

One repercussion of the loss of HIPAA-protected data is the doxing of individuals, potential blackmail and the sale of PHI data to other criminals. The data also can lead to very effective spear phishing attacks. Healthcare facilities that are targeted by criminals also need to be on the lookout for ransomware planted on their systems. In recent years we have seen many ransomware attacks targeting healthcare providers. The FBI reports that there were 59 such attacks during the first 10 months of 2020, disrupting up to 510 healthcare facilities.

CONCLUSIONS AND RECOMMENDATIONS

> **"Data can also be breached when physical devices are stolen. Computers and other electronics that contain protected information should be kept in locked rooms in secure areas.**
>
> **— VP of IT, Europe**

Ultimately, protecting health data is not unlike protecting any other type of data; the key difference is the massive fines and penalties associated with organizations where PHI is compromised. Although best practices for protecting data are widely available, sometimes common sense is the best place to start.

Foundational security, such as that provided by secure DDI (DNS, DHCP and IPAM), can supplement common-sense approaches, plug gaps that other solutions miss and extend network security from the core to the edge. This type of security is especially important in an age of remote work. Secure DDI offerings can help facilitate and secure the move to a work-from-home/remote workforce in the highly regulated healthcare industry.

For example, if PHI is stored on a laptop, thumb drive or medical device, simply purge the device of any unneeded information as soon as possible. Any PHI that is not required at the moment is a vulnerability and should be eliminated—not just deleted but overwritten and wiped away. Many medical devices can store considerable amounts of data and attackers know that. CISOs and security pros need to remember that not all computing devices are computers.

Network segmentation with varying amounts of built-in security is another common-sense method of segregating PHI. The further PHI can be stored from an Internet-facing node the better. Air-gapping might seem like an extreme action to

> **Remote workers are using IT systems that are vulnerable to phishing and malware and many are unaware of how to spot such activities until it is too late.**
>
> — IT director, Europe

take but even some air-gapped systems can be accessed and compromised if they have Bluetooth, WiFi or other wireless technologies enabled. Remember that when maintaining an inventory of connected medical devices, include remote patient monitoring devices, implanted medical devices such as pacemakers and telemetry systems used to monitor and report patient information.

Even basic actions such as software and operating system updates can help protect devices. While certifying that new OS versions will not break existing software is essential, so too is patching. Security pros need to ensure that patches are vetted and applied quickly before vulnerabilities can sneak in.

DDI can play an important role in protecting the remote workforce. It protects remote users by moving DDI controls and management to the cloud, off-loading the on-premises servers from that responsibility save for a lightweight physical or virtual appliance on premises. It also can integrate with Microsoft 365, further protecting the remote workforce.

For work-from-home medical employees, protecting data can be challenging. Again, basic cyberhygiene must be employed. Updating firmware in home routers, making sure security software is up to date and enterprise-class for protecting data, providing network segmentation hardware to keep patient data separate from family computing activity, using password managers and disabling potentially vulnerable tools, such as WiFi Protected Setup (WPS) on routers, can reduce potential security breaches on networks the IT team cannot control directly.

Cybersecurity Guidelines for Healthcare Organizations

The U.S. Department of Health and Human Services (HHS) published guidelines in 2020 after the outbreak of COVID-19 to help remote healthcare workers create a secure environment. The report, Securely Teleworking in Healthcare, published as part of the HHS Cybersecurity Program, is an invaluable asset that provides detailed information about how to secure the remote workplace, including suggestions on how to implement and expand a telework program, policy modification considerations and a description of what exactly PHI is and the laws that address how to protect it.

Below are some additional guidelines to protect both your network and remote PHI:

- Use advanced DNS protection to defend against the widest range of DNS-based attacks.
- Use a DNS firewall that automates malware protection.
- Detect and prevent data exfiltration by employing DNS-based analytics.
- Use a centralized, cloud-managed, provisioning, management and control solution, designed with the modern borderless enterprise in mind. This is what is needed to eliminate the management complexity and bottlenecks of the traditional branch office DDI. (DDI is the integration of Domain Name System, Dynamic Host Configuration Protocol and IP address management into a unified service or solution.)
- Deploy a virtual DDI appliance on a public or private cloud, which can enable you to deploy robust, manageable and cost-effective appliances.
- Have incident response and backup plans. Test the plans on a regular basis and adjust as necessary.
- Follow a consistent security policy across all platforms. For example, if you are leveraging cloud services, ensure they are secured as you would on premises.
- Implement a zero trust mobile security model.
- Ensure that you are actively monitoring and managing DNS within your organization.
- Use comprehensive threat intelligence to proactively block malicious DNS threats.
- Monitor and manage the behavior of DNS in your environment. Black-lists are not enough; you need to ensure that the protocol is behaving appropriately.
- Restrict use of DNS over TLS (DoT) and DNS over HTTPS (DoH) on assets and on the network.
- Know where your users (assets) are going from a DNS perspective, no matter where they are located (on premises, working remotely, etc.). Have a 360-degree view of all assets.
- Automate responses where possible to leverage your current infrastructure. There is no silver bullet when it comes to security, but you can solidify your posture by using defense in depth and automation.
- When PHI is sent off the secure corporate network, ensure that the data is fully encrypted end to end and the offsite user, whether an employee, contractor or partner, has a secure network that meets your compliance standards.
- Ensure that basic cybersecurity tools are in place for remote workers, including antivirus/antimalware software, firewalls, virtual private networks, multifactor authentication and ongoing cybersecurity training.

METHODOLOGY

The data and insights in this report are based on a survey conducted in October and November 2020 by CyberRisk Alliance Business Intelligence among 790 IT professionals working in the healthcare industry. The study was underwritten by Infoblox. Questions in the survey focused on cloud-computing challenges, which in recent months have been closely related to pandemic-related issues. They also addressed questions about financial losses and network business continuity issues.

Respondents were employed at large healthcare organizations with at least 1,000 employees in the United States, Latin America, Europe and Asia/Pacific. Respondents held IT and IT security roles at C-level (30%), VP (30%), director (21%) and manager (19%) levels. Virtually all respondents (91%) described themselves as either significant or final decision makers of cybersecurity budgets or operations at their organizations.

ABOUT CYBERRISK ALLIANCE

CyberRisk Alliance is an information services and business intelligence company serving the cybersecurity community. Our mission is to bring the community together to share knowledge and insight and find innovative solutions to the biggest challenges we face today. We build proprietary content, research and data, and leverage a deep network of industry experts, policy makers and senior-level practitioners to provide unique insight to our rapidly expanding community of cybersecurity professionals. We deliver our content through events, research, media and virtual learning. Our brands include SC Media, InfoSec World, CRA Business Intelligence, Cybersecurity Collaborative and Cybersecurity Collaboration Forum.

CRA Business Intelligence is a full-service market research capability focused on the cybersecurity industry. Drawing upon CRA's deep subject-matter expertise and engaged community of cybersecurity professionals—along with a world-class market research competency—CRA Business Intelligence is unique in the industry. These components together enable delivery of unparalleled data and insights anchored in our community of cybersecurity professionals and leaders eager to share their perspective on the industry's most important concerns.

More information is available at www.cyberriskalliance.com.

ABOUT INFOBLOX

Infoblox delivers the next-level network experience with its Secure Cloud-Managed Network Services. As the pioneer in providing the world's most reliable, secure and automated networks, we are relentless in our pursuit of next-level network simplicity. A recognized industry leader, Infoblox has more than 9,500 customers, including 350 of the Fortune 500.

Learn more at www.infoblox.com.

CyberRisk Alliance
Business Intelligence Resources

Infoblox
NEXT LEVEL NETWORKING