A CYBERSECURITY INSIGHT REPORT

Firms Face Financial Losses and Reputational Damage from Cloud Network Attacks and Data Breaches

Global Financial Services Sector | May 2021

Produced by CyberRisk Alliance for Infoblox

CRA | Business Intelligence

Infoblox NEXT LEVEL NETWORKING

CONTENTS

EXECUTIVE SUMMARY

> **We encountered a cyberattack, which led to the paralysis of the entire system.**
>
> — VP of IT, Europe

Financial services firms face a host of challenges in protecting their users' data. Regional compliance regulations and laws relating to financial services, as well as cybersecurity concerns relating specifically to the sector, all make network security especially complex. Add in the challenges and vulnerabilities introduced by the COVID-19 pandemic, along with the business process changes, and the financial services sector ended up facing serious difficulties throughout 2020 and continues to do so in 2021.

The regulatory landscape is especially complex. Financial services companies need to deal with a myriad of compliance rules, regulations and laws. On the international front, there are laws such as the General Data Protection Regulation (GDPR), which deals, in part, with holding or processing personally identifiable information (PII) of a European Union citizen anywhere in the world. Financial services companies also need to be concerned with national privacy laws, such as Law 13.709 of Brazil or the General Law for the Protection of Personal Data. In the United States, companies doing business in California must comply with the California Consumer Privacy Act (CCPA) and the recently passed California Privacy Rights Act (CPRA), along with dozens of other state regulations.

There are even laws at the local level. New York City, for example, enacted NYDFS Cybersecurity Regulation (23 NYCRR 500) that focuses on banks, lenders, mortgage companies, insurance companies and service providers. On top of that, industry-specific regulations, such as the Payment Card Industry Data Security Standard (PCI DSS), which dictates how companies that process credit and debit cards protect PII, impact companies globally. At every level there are requirements that

sometimes conflict with other laws and regulations, creating an ever-growing challenge for security pros and risk officers in this market segment.

This report takes a global view of the financial services 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 financial services industry faces, the solutions companies are deploying to defend themselves and the spending these require.

Among the report's findings for financial services companies worldwide:

- IoT attacks, cloud vulnerabilities and misconfigurations and attacks to manipulate data/statistics are the top cyberthreats financial services professionals expect to confront in the next 12 months, each cited by more than half of respondents worldwide.

- Data breaches were the top attack vector against cloud networks in the past 12 months, cited by 54% of respondents.

- Worldwide, financial firms that experienced a data breach reported estimated average losses of $4.2 million from these attacks with U.S. organizations experiencing the highest, at $4.7 million. Victims of network outages lost an estimated $3.2 million overall with the highest average losses among firms in the Asia/Pacific region ($4.3 million).

- Globally, the most effective mitigation tactics were network monitoring (76%), threat intelligence (64%) and threat hunting (57%).

- Overall, the estimated average costs for preventing breaches and network outages was roughly $4.8 million, with the highest estimates from U.S. firms at $5.3 million.

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.

In the real world of financial services, the attacks and their repercussions can take years to resolve and have long-lasting implications. Late last year, for example, a federal grand jury for the Western District of Pennsylvania indicted six Russian military intelligence officers for their roles in the NotPetya malware attacks from 2017. The indictments were part of a long-running investigation into the state-sponsored attacks against critical infrastructure providers, including some in the financial sector, that ended up costing the victims billions of dollars.

Focusing directly on financial services, the FBI's Internet Crime Complaint Center (IC3) also reported last year that the increased use of mobile banking applications could lead to increased exploitations. In the first half of 2020 alone, the FBI said, the use of mobile apps increased 36%.

> **We are constantly updating and verifying our systems so that we are always at the forefront of any hacker attack, and we handle financial information from many customers so it is more than essential to have efficient security.**
>
> — IT director, Latin America

"When the attackers successfully compromise accounts, they monetize their access by abusing credit card or loyalty programs, committing identity fraud, or submitting fraudulent transactions such as transfers and bill payments," according to a 2020 FBI financial services industry notification. Citing an unsourced data analytics report, the notification also states 60% of users employ one or more passwords across multiple accounts, with credential stuffing attacks correlating to an increase in leaked credentials across the dark web.

Earlier this year, the European Banking Authority (EBA) disclosed it had been affected by the cyberattack against Microsoft Exchange Servers. As a precautionary measure, the EBA was forced to take its email systems offline for several days during the attack. The organization said it was possible that personal information was disclosed during the attack. Microsoft attributed the widespread Exchange Server attacks to the state-sponsored hacking group Hafnium, operating out of China.

This report probes financial services 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. Other breach-related costs include recovery and mitigation expenses, additional network security fees such as hiring consultants and forensics experts to evaluate and penetration test the rest of the network to identify potential vulnerabilities, 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.

CYBERSECURITY THREATS/ATTACKS

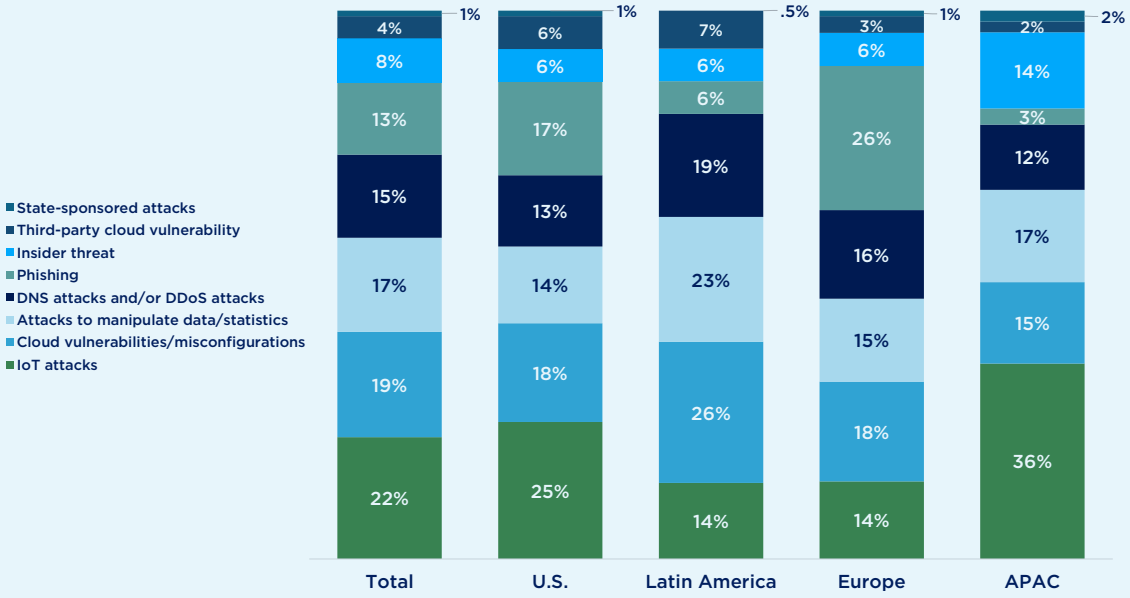
> **...risk is compounded by the nature of business adopting IoT technology.**
>
> — CISO, U.S.

Financial services firms worldwide will face a variety of IT security threats in the coming year. Among the top threats that industry security professionals anticipate are IoT attacks (22%), cloud vulnerabilities (19%) and attacks to manipulate data or statistics (17%). IoT attacks are top threats for both U.S. (25%) and Asia/Pacific (36%) firms. In Europe, more than one in four firms (26%) say phishing will be their top threat, and Latin American firms believe their top threats will be cloud vulnerabilities and misconfigurations (26%).

When asked directly, many respondents commented about fighting off constant phishing attempts, and a VP from a U.S. firm added that the "increase in the spoofing and phishing to their aging and vulnerable customer bases was a chief concern."

Top IT Security Threats

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



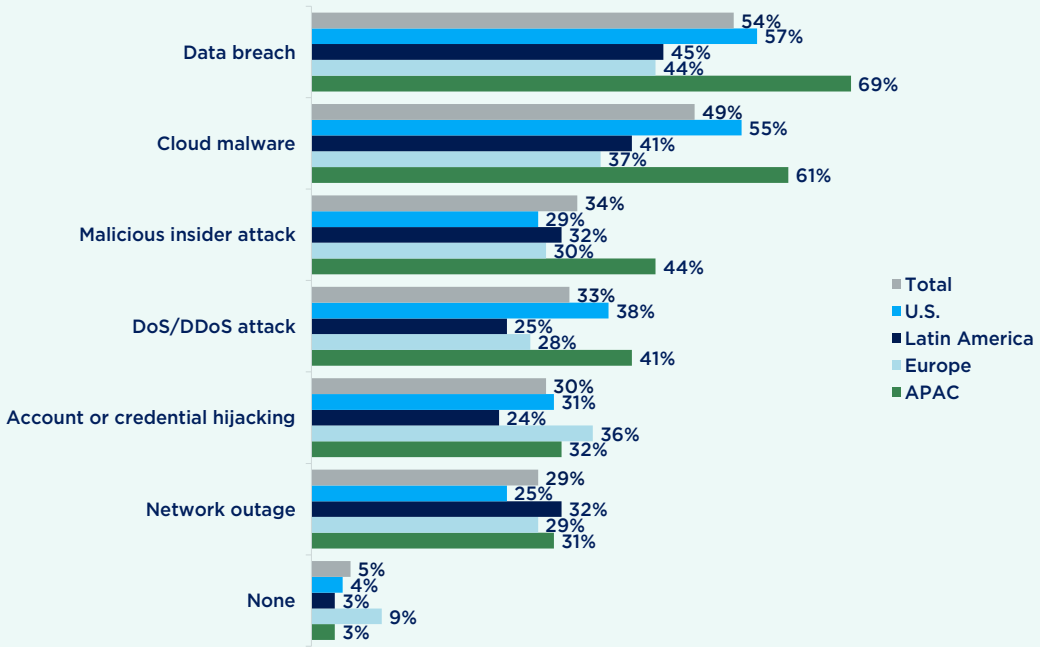
> **The concern my organization has for the next 12 months is data manipulation and customer data security.**
>
> — CISO, U.S.

More than half of all firms (54%) reported they were hit by data breaches during the previous 12-month period, while nearly half (49%) encountered cloud-based malware attacks. Asia/Pacific firms were the hardest hit across the board, falling victim to more cloud networking attacks as a whole than firms in any other region, with data breaches (69%), cloud attacks (61%) and insider attacks (44%) being the most prevalent.

Cloud malware isn't a new threat and since it exists outside the enterprise network and beyond the firewall, many firms said they are concerned about the security and integrity of their data as they migrate their data to public and third-party clouds in the medium to long term.

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

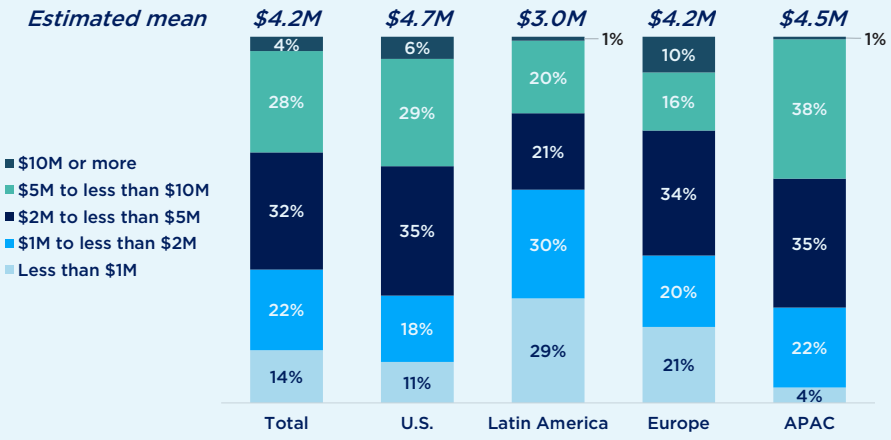
> **We have adopted saving our files in a private cloud to avoid any loss of our important data, and we encrypt our system to prevent possible intrusions.**
>
> — IT director, Latin America

Overall, financial firms that experienced a data breach reported an estimated average loss of roughly $4.2 million from these attacks, with U.S. organizations,experiencing the highest estimated average losses at approximately $4.7 million. Victims of network outages lost an estimated $3.2 million on average, with the highest losses among firms in the Asia/Pacific region (roughly $4.3 million).

It is easy to understand how a data breach can impact corporate network operations and profits, but unscheduled network outages can be more challenging. Even if the outage is due to non-malicious interaction or perhaps as collateral damage to an attack on another company, the consequences are the same as from a targeted attack. For example, the harm is still

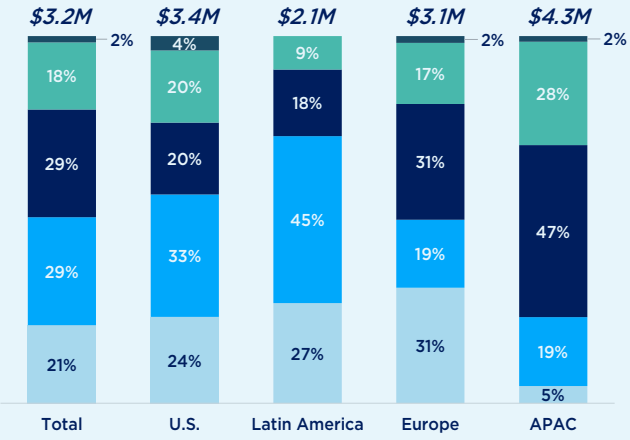
Data Breach Financial Losses

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



Network Outage Financial Losses

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



Notes:
Percentages may not sum to 100% due to rounding.
Estimated mean losses were calculated using the midpoint value for each range ($15M was used for the midpoint value for the upper range of "$10M or more"). See the Methodology section for more details on this calculation.

> **...the breach of our customer data security would lead to major financial losses.**
>
> — IT director, Latin America

just as real and costly when a multi-tenant cloud server is taken down because someone from another company introduced malware that impacted the server's operating system or other server-wide service such as the hypervisor. In fact, cloud-based outages often are not the fault of the companies that suffer significant network outage costs.

Of course, a network outage due to an attack on the company's on-premises network or cloud service provider also will impact corporate operations, revenue, expenses and the like and could be due to an employee's bad decisions or perhaps an insider threat, but that falls under the category of threats to be defended against through training, products or services. Sometimes bad things simply happen and the company needs to respond.

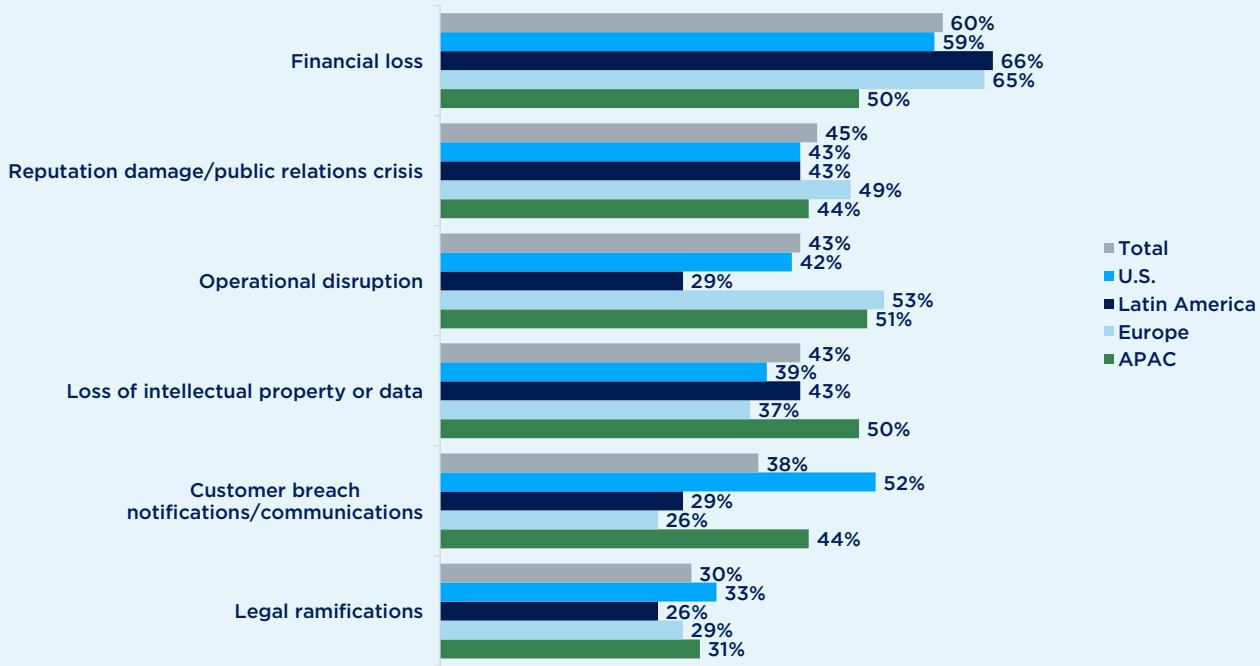
The top impacts of network outage attacks for financial services firms are financial losses, reported by 60% of all organizations, with slightly more Latin American (66%) and European (65%) firms expecting financial losses as a top consequence of a network outage. Reputational damage/public relations crisis was considered the next greatest impact of these types of attacks, mentioned by 45% of all respondents, with only a slight variance across regions. Operational disruption (reported by 43% overall) was high on the list for European (53%) and Asia/Pacific (51%) firms. Loss of intellectual property or data was reported by 43% of all respondents, followed by customer breach notifications and legal ramifications (38%). Among these, more than half of U.S. firms (52%) deem customer breach notifications a top consequence of a network outage attack.

> **I believe that all financial services companies should invest heavily in data security, given the fact that this problem, in addition to causing financial losses, can damage the organization's credibility.**
>
> — IT manager, Latin America

When asked about specific disruptions from a network outage attack to their organization, respondents described customer disruptions at bank branch locations, the wait time for a new bank card activation after a data breach, insurance firms' inability to process claims in a timely manner and the risks of reputational damage to their firm.

Top Impacts of a Network Outage

What do you think are the greatest potential impacts or consequences to your organization from a network outage?



RISK MITIGATION AND SPENDING

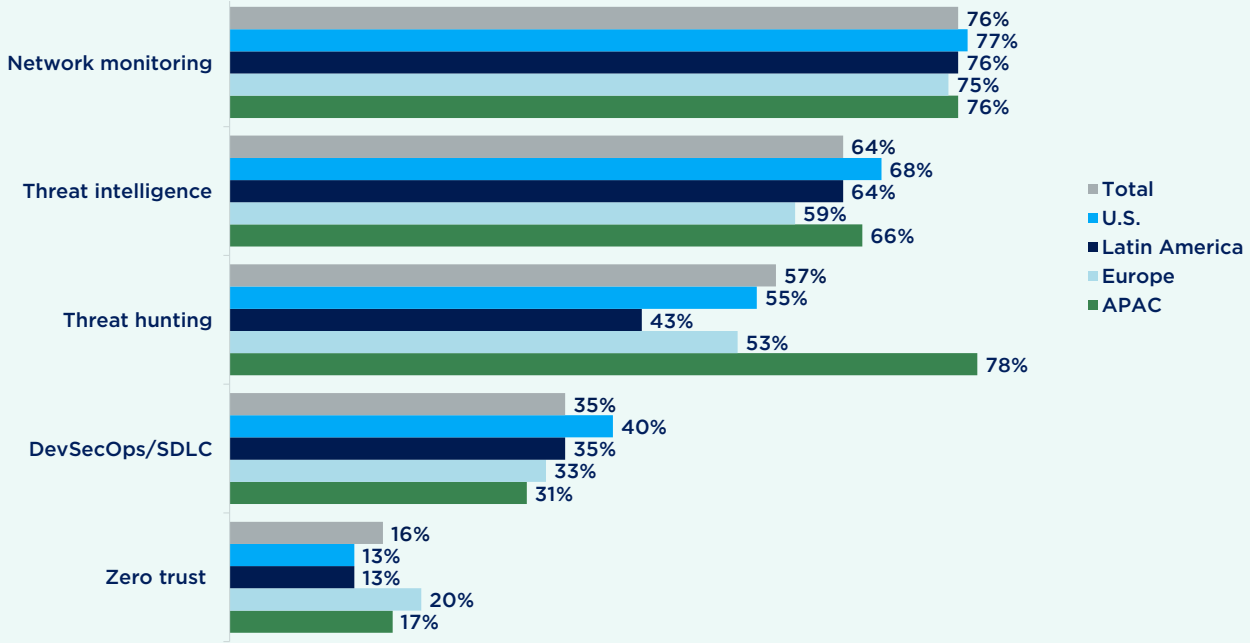
> **We need to migrate to the cloud. These DDoS attacks delay many operations and irritate customers.**
>
> — VP of IT, Latin America

By far, the mitigation tactic of choice was network monitoring as reported by more than three out of four (76%) respondents overall (with negligible differences by region). Threat intelligence was another top tactic, cited by nearly two-thirds (64%) of all respondents.

Most notably, a large majority (78%) of Asia/Pacific firms mentioned threat hunting as their top mitigation tactic, which was significantly higher than in other 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)



> **Cloud misconfiguration may be the security concern for us in the next 12 months.**
>
> — CISO, Asia/Pacific

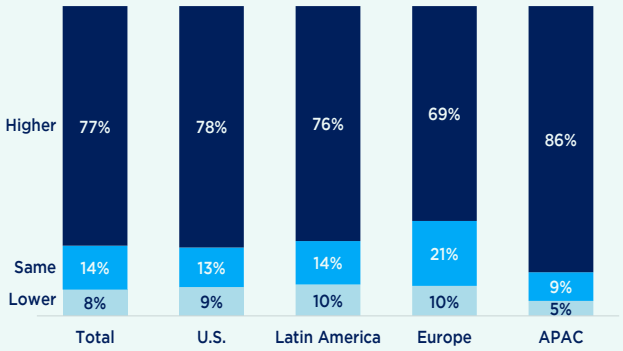
The survey also found that spending for 2020 was expected to be higher than 2019 due to the COVID-19 pandemic. Financial firms confirm they face attacks of increased complexity and scope and on average, more than three of out four (77%) respondents say they increased spending in 2020 compared to the prior year, with the largest proportion (86%) coming from Asia/Pacific firms. The outlook for 2021 is no different — the vast majority of firms (82%) expect their spending to rise again, with a significantly higher proportion of firms in Asia/Pacific (90%).

Globally, the estimated average costs for preventing breaches and network outages were roughly $4.8 million, with the highest estimates from U.S. firms at $5.3 million.

Overall, firms worldwide face a long list of challenges in protecting their organizations from IT security threats and breaches. At the top of the list are cloud-related issues and network outages, with roughly 40% of all firms worldwide indicating they face these difficulties in protecting their firms. 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 also key challenges to firms worldwide.

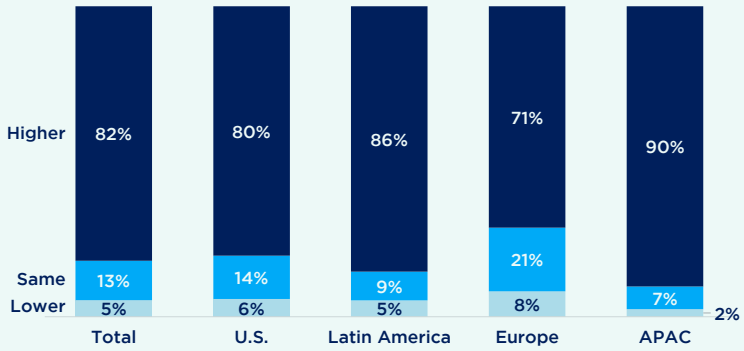
2020 IT Security Budget or Spending Compared to 2019

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



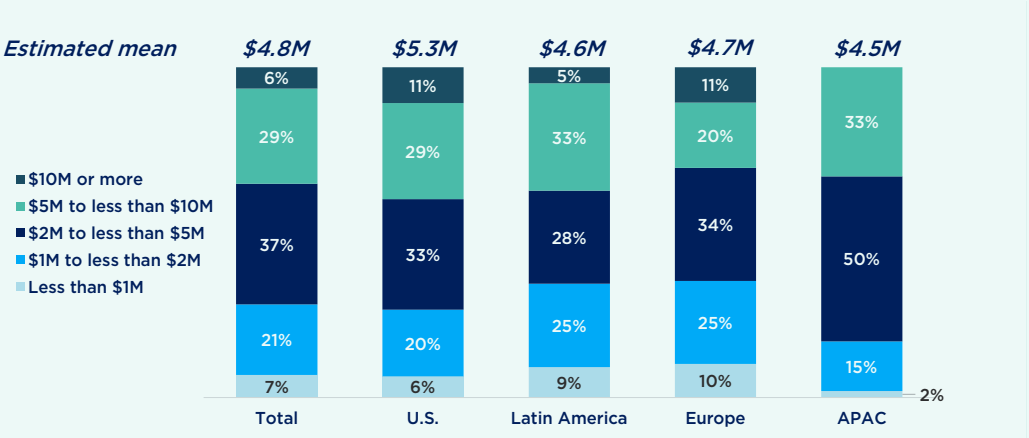
Change in IT Security Budget or Spending in 2021

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



Projected Costs for Preventing Breaches and Network Outages

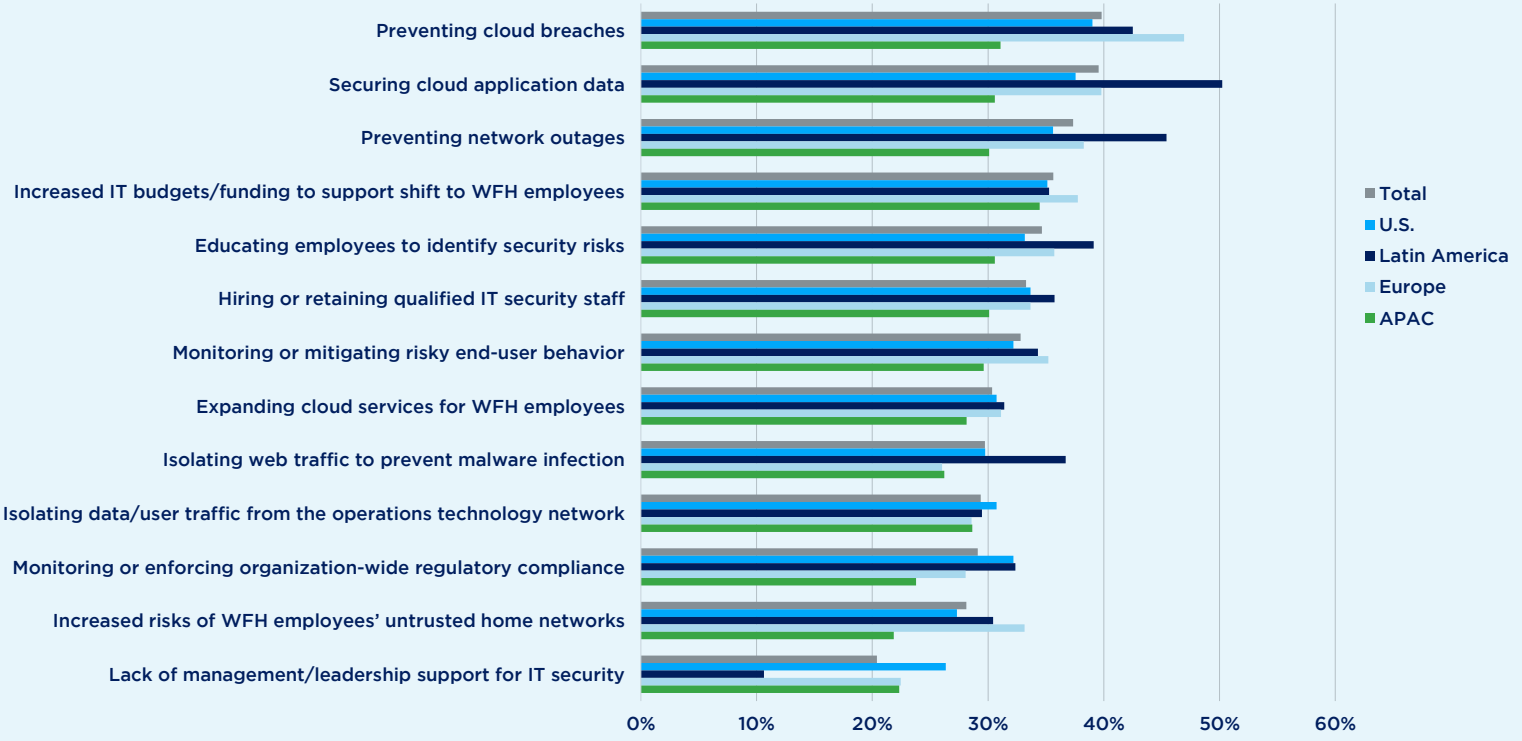
What do you estimate will be your organization's average costs over the next 12 months for the prevention of breaches and network outages?



Notes:
Percentages may not sum to 100% due to rounding.
Estimated mean costs were calculated using the midpoint value for each range ($15M was used for the midpoint value for the upper range of "$10M or more"). See the Methodology section for more details on this calculation.

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

Security teams need to be perfect 100 percent of the time, while bad actors only need to get lucky once.

Financial services companies have always been the targets of bad actors wanting what was not theirs. Whether it was Sextus Pompeius, a Roman pirate from 44 BC; Billy the Kid, a bank robber in the Old West during the 19th century; Harvey John Bailey, a 1920s-era criminal known as the Dean of American Bank Robbers; or the hackers of today who steal millions using phishing, ransomware and other cyberattacks, stealing other people's money is a long-standing and common criminal activity.

Defending against such threats requires a full range of offensive and defensive techniques. One effective technique uses a centralized, cloud-managed provisioning, management and control solution, designed with the modern borderless enterprise in mind to eliminate the management complexity and bottlenecks of the traditional branch office. The technology is called DDI, the integration of Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP) and IP address management (IPAM) into a unified service or solution.

DDI brings together these key technologies, giving networking administrators visibility and control over the network. These components enable virtual machine discovery to automate inventory management in cloud environments, give software-defined networks the ability to identify the closest Internet breakout and enhance remote site survivability and leverage containerization to protect cloud-native apps and enhance DevOps. Additionally, DDI includes a software-defined perimeter that supports network identity and context for policy rules and their enforcement in security orchestration, automation and response (SOAR); security information and event management (SIEM); cloud access security brokers (CASBs); zero trust; next-generation firewalls and more; plus the enabling and diverse array of the Internet of Things, including 5G devices, artificial intelligence and machine learning, industrial IoT, and both IT and operational technology (OT) on-prem networks.

...if one rule says a breach must be reported within 90 days and another says within 72 hours, then the pragmatic approach would be to report all breaches within 72 hours.

Compliance requirements are a big part of the cybersecurity concerns for the financial services sector. The far-reaching requirements of the European Union's General Data Protection Regulation (GDPR), combined with various state and federal regulations in the United States, plus the international PCI DSS standard for bank cards, make this segment one of the most highly regulated with conflicting rules and a challenging market for security pros. (PCI DSS is highly prescriptive in its approach, while GDPR is intent-based and can clash with PCI DSS.)

Perhaps the best approach for CISOs is to adhere to the strictest components of each regulation. For example, if one rule says a breach must be reported within 90 days of discovery and another says within 72 hours, then the pragmatic approach would be to report all breaches within 72 hours. While this might seem extreme, it is one way to ensure compliance.

RECOMMENDATIONS & GUIDELINES

Organizations in the financial services sector include but are not limited to banking, insurance, mortgage and other lenders and securities brokers. The sector has one of the biggest targets on its back for cyberattackers because of the vast amounts of money and data these organizations handle. Below are some guidelines for protecting networks and data in financial services organizations.

- 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 utilizing DNS-based analytics
- Use a centralized, cloud-managed, provisioning, management and control solution, designed with the modern borderless enterprise in mind. This is necessary to eliminate the management complexity and bottlenecks of the traditional branch office DDI
- Deploy a virtual DDI appliance on a public or private cloud, which can enable you to simplify delivery of robust, manageable and cost-effective DDI services
- Have an Incident Response and Backup Plan. Test the plan on a consistent basis and adjust as necessary
- Have a consistent security policy across all platforms. For example, if you are leveraging cloud services, ensure they are secured as you would on premises
- Ensure 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 as appropriate
- 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

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 814 IT professionals working in the financial services industry. The study was underwritten by Infoblox. Questions in the survey focused on cloud-computing challenges, which in recent months have been closely associated with pandemic-related issues. They also addressed questions about financial losses and network business continuity issues.

Respondents were employed at large financial firms with at least 1,000 employees in the U.S., Latin America, Europe and Asia/Pacific. Respondents held roles at IT and IT security in C-level (30%), VP (30%), Director (21%) and Manager (19%) levels. Virtually all respondents (94%) described themselves as either significant or final decision makers of cybersecurity budgets or operations at their organizations.

Note: Estimated means are reported for "Data Breach Financial Losses," "Network Outage Financial Losses" and "Projected Costs for Preventing Breaches and Network Outages" in addition to ranges/intervals, which were presented to respondents in the survey. Means were calculated by multiplying the midpoints for each range ($15M was used as the midpoint value for the upper range of "$10M or more") by the frequencies of each of the corresponding ranges. The sum of the products was then divided by the total number of values to derive the mean and should be considered a "ballpark" average due to the arbitrary midpoint for the upper range ($10M or more) used in the calculation.

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 is the leader in modern, cloud-first networking and security services. Through extensive integrations, its solutions empower organizations to realize the full advantages of cloud networking today, while maximizing their existing infrastructure investments. Infoblox has over 12,000 customers, including more than 70% of the Fortune 500.

Learn more at www.infoblox.com

CRA | Business Intelligence
A CyberRisk Alliance Resource

Infoblox
NEXT LEVEL NETWORKING