A CYBERSECURITY INSIGHT REPORT

Local, State and Federal Agencies Gear up to Fight Cloud Network Attacks and Data Breaches

U.S. Government Sector | January 2021

Produced by CyberRisk Alliance for Infoblox

CyberRisk Alliance
Business Intelligence Resources

Infoblox®
NEXT LEVEL NETWORKING

CONTENTS

EXECUTIVE SUMMARY 3

INTRODUCTION 4

CYBERSECURITY THREATS/ATTACKS 5

COSTS AND IMPACTS OF DATA BREACHES AND NETWORK OUTAGES 7

RISK MITIGATION AND SPENDING 9

OTHER AREAS OF CONCERN 13

THE IMPACT OF COVID-19 16

SOLUTIONS 18

CONCLUSIONS AND RECOMMENDATIONS 20

METHODOLOGY 23

ABOUT 24

EXECUTIVE SUMMARY

> **Using technology and accessing our database remotely is happening at a much higher frequency than ever before due to the pandemic.**
>
> **— IT manager, state government**

While working in the public sector and private sector have many differences, one characteristic is similar: cybersecurity and threats. Both sectors feel the pain of not having a sufficient community of trained and available security staff to hire, both are constant targets of phishing and related social engineering attacks and both are trying to balance the three-pronged attacks of the pandemic, the relocation of employees to work-from-home status and increased risks from attacks on cloud assets.

The insights in this report are based on a survey conducted in October and November 2020 by CyberRisk Alliance Business Intelligence among 294 senior-level federal, state and local government IT executives. 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.

INTRODUCTION

> **State-sponsored cyberattacks by countries can disrupt communications, military activities, or other services that citizens use daily.**
> — CISO,
> local government

Government entities at all levels are facing significant challenges as they try to realign personnel and assets due to the work-from-home phenomenon brought on by the COVID-19 pandemic. According to a U.S. Bureau of Labor Statistics study for 2017 to 2018, just 15% of workers worked from home before the pandemic, while 32% of state government workers did so. Today, the percentage of employees working from home is closer to 80% or more.

This is not the first time a national emergency forced workers to leave their corporate facilities and move into home offices. Telework spiked after both the 9/11 terrorist attacks and the anthrax attacks soon afterwards. The current pandemic, however, is international in scope and impacts far more workers worldwide.

Today, governmental agencies are expanding plans to support their work-from-home employees even as federal employees are told they will have to return to work shortly. A survey by Government Business Council, the research arm of *Government Executive*, found that nearly three-quarters of federal government employees are telecommuting and almost two-thirds of them (63%) are full-time employees.

According to *American City & County*, a publication dedicated to local and state government coverage, 61% of local municipalities allow their employees to work from home, although some employees are required in the office simply to process mail and file papers.

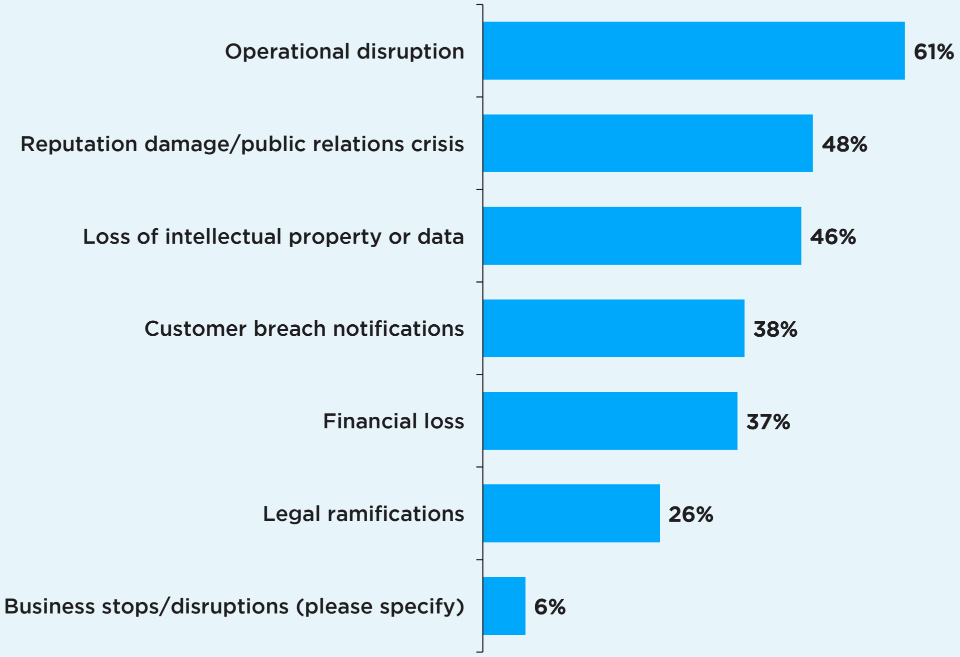
CYBERSECURITY THREATS/ATTACKS

> **As a government agency with sensitive data, we receive a lot of phishing emails from cyber criminals that pose as legitimate internal or external emails asking our employees to enter their credentials or other sensitive information.**
>
> — IT manager, federal government

As employees work from home, security is compromised on all fronts. That was the general sentiment echoed across the majority of government IT security professionals in this study. By far, the most serious issue government respondents said they face are the ever-present phishing attacks and the potential for disclosure of sensitive information, as reported by 24% of all survey respondents. Next are data-related attacks (19%) followed by cloud vulnerabilities and misconfigurations (18%).

Top IT Security Threats

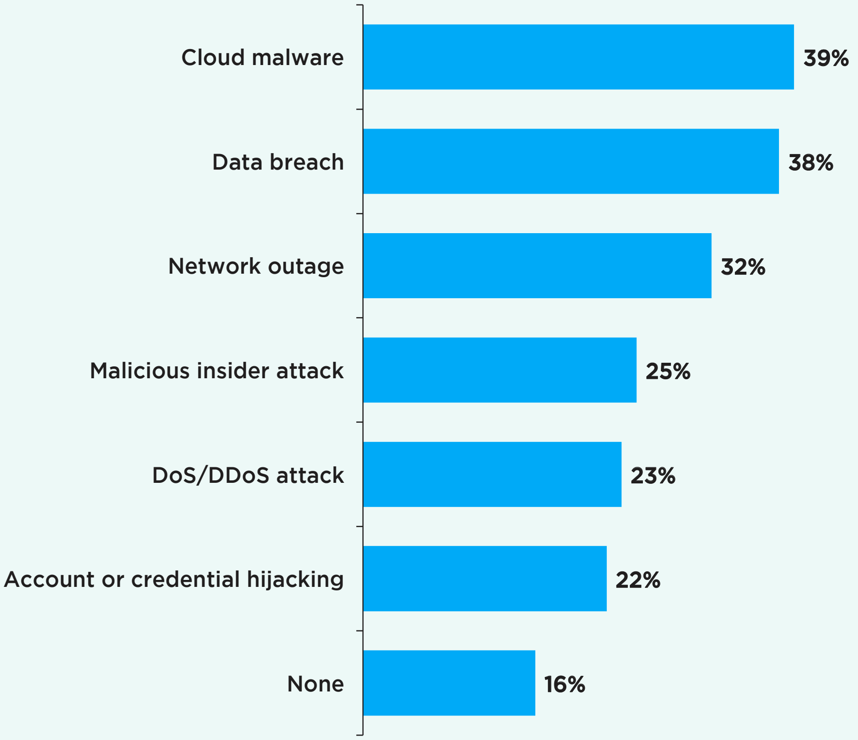
In your opinion, which of the following is your organization's top IT security threat in the next 12 months?



When asked about attacks respondents experienced in just the past 12 months, the vast majority (84%) reported one or more cloud networking attacks. More than one-third reported they were hit with cloud malware (39%) or a data breach (38%) while nearly one-third (32%) suffered a network outage. One in four respondents encountered malicious internal attacks, which can be just as destructive as well-coordinated phishing attacks.

Cloud Networking Attacks

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



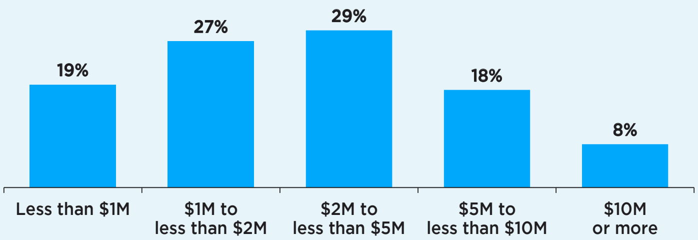
COSTS AND IMPACTS OF DATA BREACHES AND NETWORK OUTAGES

The challenge of identifying how much a company lost from a data breach is due, in part, by companies measuring losses differently. Additionally, not all of the respondents participating in this survey were privy to their organization's financial loss statistics, which in aggregate include costs such as legal fees, lost business, compliance fines, technology replacement and other direct or indirect costs to the organization.

Of those who suffered a data breach, more than half (55%) estimated their losses as at least $2 million, while 43% of network outage victims believed the cost to their government organization was $2 million or more.

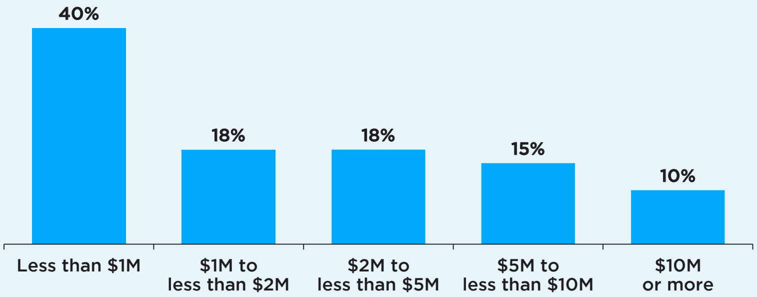
Data Breach Financial Losses

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?



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

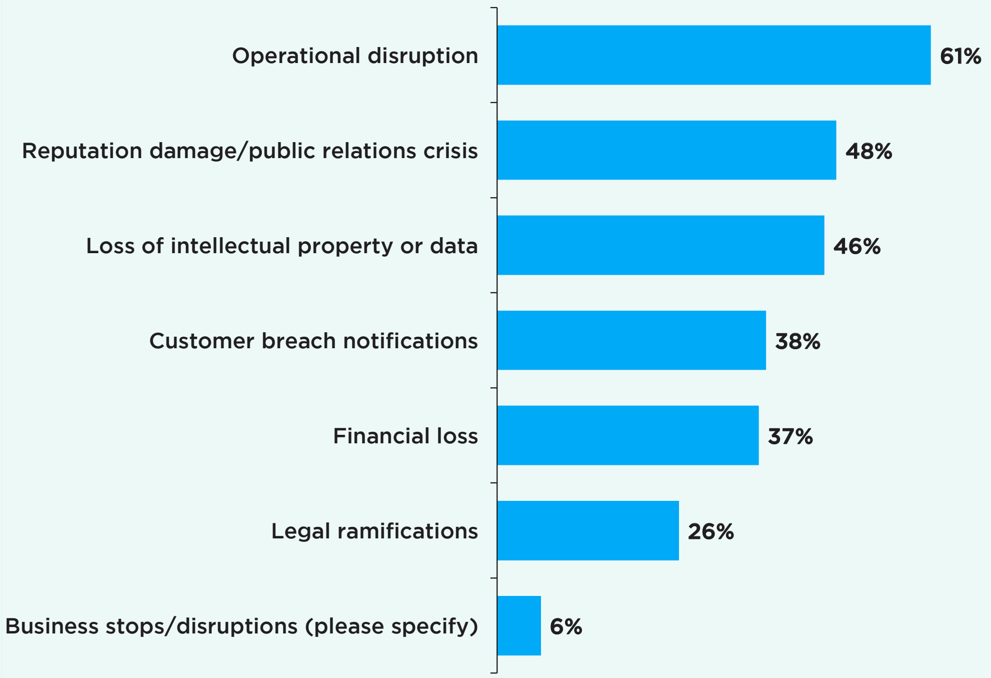
> **We are a federal public agency responsible for the reliability and security of the nation's electricity grid and gas transportation infrastructure. A disruption could have severe consequences on the country's electricity and gas infrastructure.**
>
> — IT manager, federal government

When asked what they believe are the greatest potential organizational impacts from a network outage, most respondents (61%) cited operational disruptions. Other potential consequences include reputational damage (48%) and lost intellectual property or data (46%). Additionally, 37% indicated financial losses as a major consequence.

In specifying potential business stops or disruptions as a result of a network outage, respondents described devastating outcomes such as failure of the U.S. military's supply chain management system to deliver equipment and weapon systems to troops on time; the inability of state-operated public transit systems to furnish bus and train arrival/departure times and notices; and the disabling of law enforcement video camera feeds for crime control. Others mentioned inoperable government systems such as claims processing, work order management and utility services.

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)

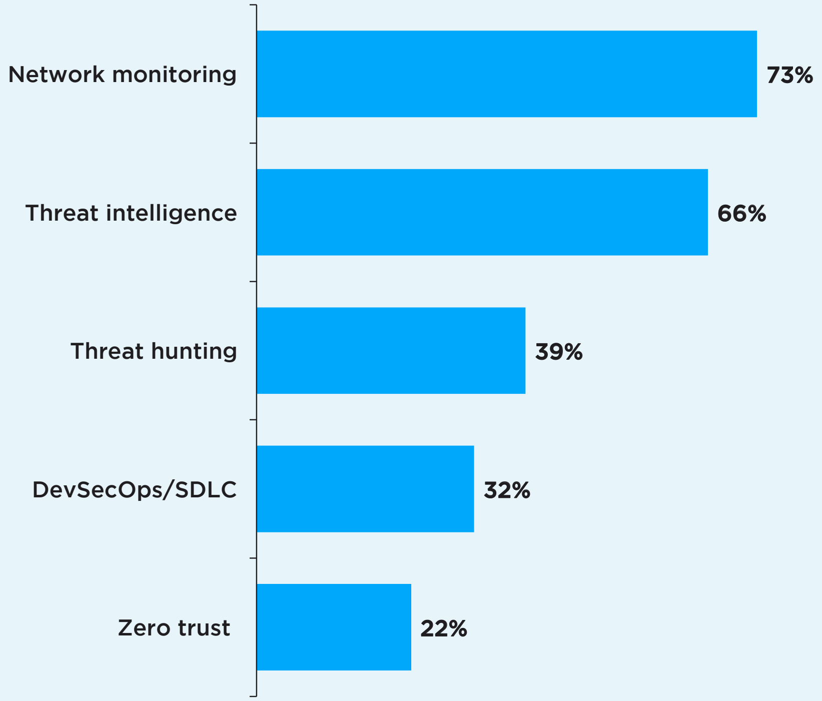


RISK MITIGATION AND SPENDING

The most effective mitigation tactics mentioned by a large majority of respondents include network monitoring (73%) and threat intelligence (66%). Popular threat intelligence feeds include those from critical infrastructure Information Sharing and Analysis Centers (ISACs), industry-specific boutique threat intelligence feeds, open source intelligence (OSINT) providers and internal security information and event management (SIEM) and other data logging systems. There are a variety of network monitoring tools as well. These include everything from performance and traffic analysis tools to intrusion and detection tools to next-generation firewalls and tools that monitor the health of attached user workstations and other computing assets.

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)



> **“Sometimes it’s hard to justify these costs to senior leadership because there is no tactile way to measure ROI. However, if you are able to explain the real costs associated with breaches — including recovery, fines, legal problems, lawsuits, etc. — they realize the potential loss is generally greater than the expenditure to mitigate the risk.**
>
> — CISO,
> federal government

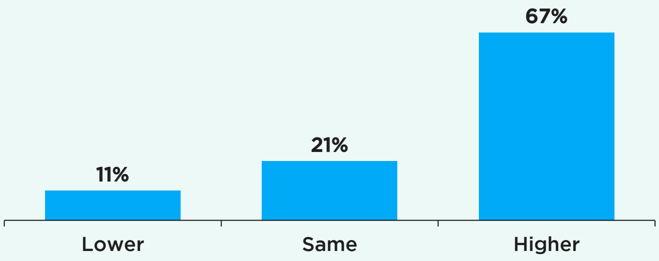
If the COVID-19 pandemic has any kind of silver lining, it would be the recognition of cybersecurity concerns. Respondents report that 2020 IT security budgets and spending were higher — sometimes significantly — after COVID-19 than before. More than two-thirds (67%) indicated their government organization had increased its IT budget in 2020, and most (73%) expect it will increase in 2021.

The cost of data breaches is well documented. According to a 2020 report from Ponemon, the average cost of a data breach is $3.86 million. Some 27% of survey respondents said they expect to spend from $2 million to $5 million to prevent breaches and network outages. Considering the average costs of a data breach, these proactive expenditures are sound investments in preventing data breaches that could spell disaster for government organizations.

It should come as no surprise that a top challenge cybersecurity managers face today is hiring and retaining qualified IT security staff — 38% identified that as their top issue. Other top pain points include preventing network outages (40%), securing cloud data (38%) and educating employees to identify security risks (37%).

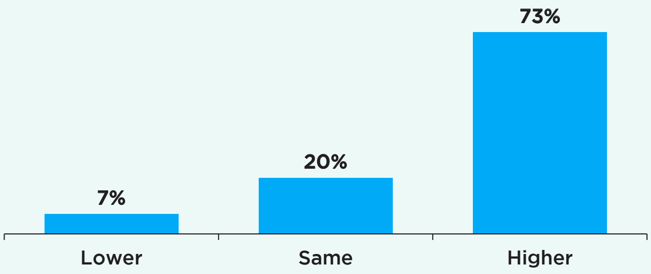
2020 IT Security Budget or Spending Compared to 2019

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



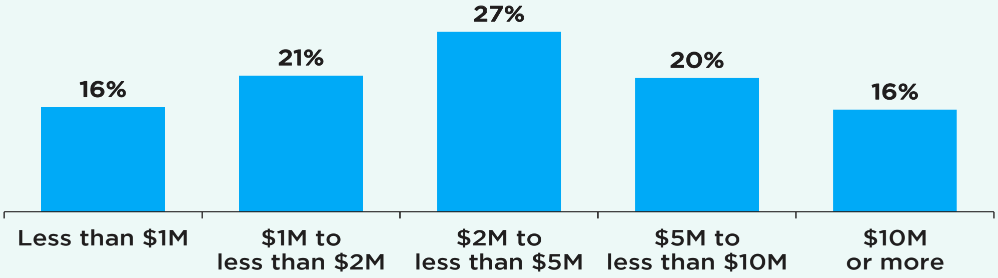
Change in IT Security Budget or Spending in 2021

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



Projected Costs for Preventing Breaches and Network Outages

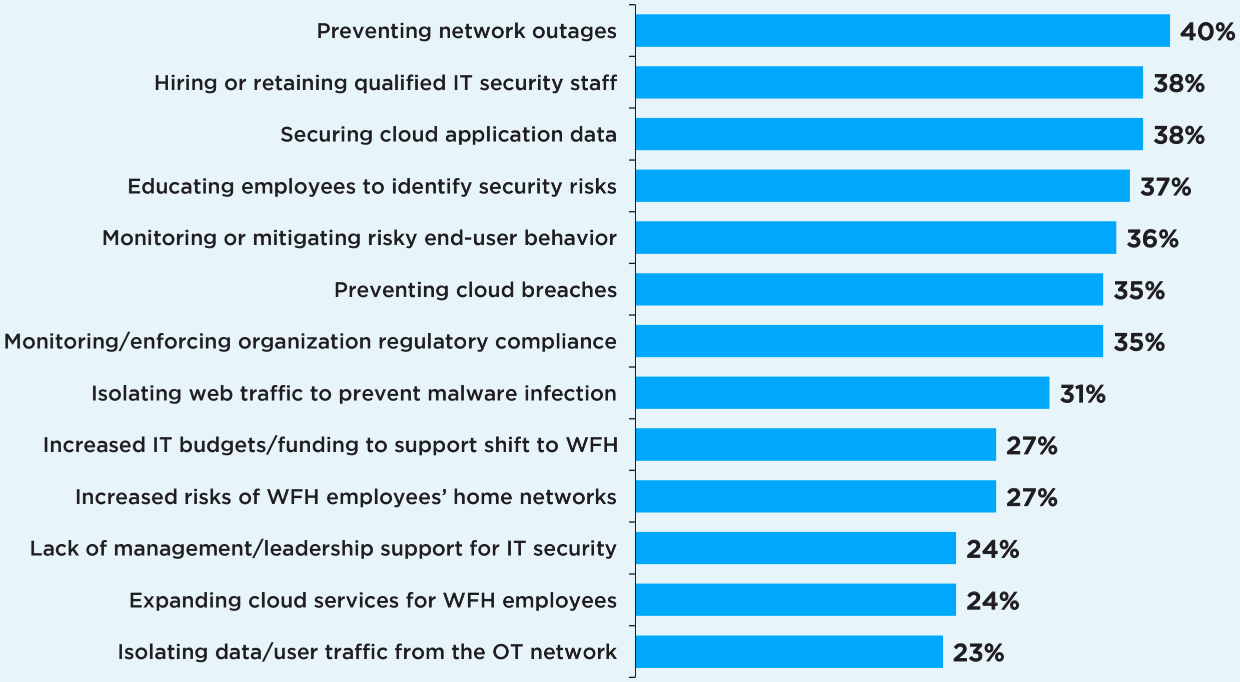
What do you estimate will be your organization's average costs over the next 12 months for the prevention of breaches and network outages?



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

> **Get compliant with NIST 800-171r2 ASAP. It covers a lot of territory. Then focus on user security and phishing awareness.**
>
> — CISO, federal government

A popular cyberattack — ransomware — is quite the double-edged sword. While ransomware attacks against government agencies are common, the victims are in a precarious situation. The question of pay versus not pay is complicated because if one chooses to pay the attackers, they run the risk of violating federal laws against sending money to potential terrorists. But potentially violating the law is not the only issue; the payment itself can be significant.



Cybersecurity Challenges

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

OTHER AREAS OF CONCERN

A 2019 article in *StateScoop* reports that public sector victims of ransomware pay almost 10 times as much money on average than their private-sector counterparts. At the time government victims were paying on average $338,295, while private-sector victims paid $36,295.

Public-sector victims of ransomware pay almost 10 times as much money on average than their private-sector counterparts.
— *StateScoop* (2019)

In 2020, Department of Defense contractors EWA Technologies, EWA Government Systems Inc. and Simplicikey were among companies targeted by the RYUK Ransomware. In October 2020, the FBI, CISA and U.S. Cyber Command announced that a North Korean hacking group had been conducting a cyber espionage campaign against individual experts, think tanks, and government entities in South Korea, Japan, and the United States, according to the Center for Strategic and International Studies.

Some cities chose not to pay, instead opting to follow FBI guidance to repair their networks rather than pay the criminals. Atlanta spent well in excess of the $17 million it thought it might cost, while Imperial County, California, spent far more than the $1.2 million the cyberattackers requested. A May 2019 attack against the City of Baltimore cost in excess of $18 million to remediate; the original attackers had requested a ransom of $76,000, according to published reports. The Baltimore attack was a ransomware-based attempt at data extortion, the report stated. These attacks can also be coordinated as it was in August 2019 when 23 different government entities in Texas were all hit with a ransomware attack.

Critical infrastructure also is in the crosshairs of state-sponsored cyberattackers, according to a White House report involving the National Security Agency (NSA) and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) security alert published in July 2020. Specifically, the threats are being made against electricity, water and gas facilities. The targeted systems are operational technology (OT), which often includes everything from Internet-connected sensors and systems controls to environmental controls such as heating, ventilation and air conditioning (HVAC), lighting, electronic door locks and openers and similar non-IT but Internet-connected technology throughout buildings and industrial plants.

The DHS and CISA alert specifically identified these details, identifying risks and impacts, along with recommendations on how to mitigate those risks.

The alert goes on to outline specific actions companies can take to mitigate the damage from the attack on their OT systems and ways to harden their networks. The July report followed another report from CISA in February 2020 warning of anticipated attacks on pipeline operations. That alert also offered extensive recommendations for mitigating the risk.

In October, CISA also issued an alert for local, state and federal government security teams that Emotet malware, a sophisticated Trojan that commonly functions as a downloader or dropper of other malware, resurged in July after being dormant since February. While the Emotet alert was appropriate, it followed similar alerts in other countries by nearly a month.

It was not unusual years ago for cyber-attackers to hit various government sites simply to build up “hacker street creds” to demonstrate their competence.

Emotet originally was released in 2014 and tends to be effective against older technology. Unfortunately, many state and local governments still use older hardware and software due to budget constraints, so they are more vulnerable to the malware.

Another area of concern for the federal government are cyberattacks against physical facilities, such as embassies and offices. In recent years cyber threats against embassies in Cuba and Israel garnered coverage, even if the ultimate cause of the “attacks” was never identified conclusively. Even in the U.S. political arena allegations of cyberattacks between candidates, as well as alleged attacks by and against protesters, have been made, although never proven.

It was not unusual years ago for cyberattackers to hit various government sites simply to build up “hacker street creds” to demonstrate their competence. For hackers who want to operate in the Dark Web, having published and authenticated reports of their abilities is needed for other hackers to trust they are indeed cybercriminals and not undercover law enforcement.

THE IMPACT OF COVID-19

The current pandemic is having a major impact on all levels of government. Aside from the financial impact the pandemic is having on the private sector, government IT professionals also are facing the following challenges:

- Workers are being required to work from home
- IT and security staffs must provide WFH employees with new equipment, which has major implications for IT budgets
- Users are connecting to government networks from untrusted and often compromised home networks
- Users are employing personal equipment and IoT devices to connect to government networks and clouds that might not be secured to the governmental agency's security standards

However, governments have other concerns as well. Government operations potentially can impact much larger groups of people than a corporate attack. Depending on the government entity targeted, the effect could impact critical infrastructure at all levels. The COVID-19 effect of draining critical financial resources to fund purchases of hardware and software for newly displaced employees, plus expenses for significant increases of cloud services and, in some cases, a forced digital transformation from on-premises data center to cloud-based assets, is putting a strain on both financial and staffing resources.

From the citizenry perspective, the pandemic has opened the proverbial Pandora's box of fake "official" websites devoted to COVID-19, misinformation from websites purporting to be the Centers for Disease Control and Prevention and other government and medical facilities that actually are watering holes for malware and ransomware attacks on hospitals delivered in emails purporting to be information about COVID-19.

MALWARE CYBERSECURITY HYGIENE TIPS:

- Apply the latest patches to your hardware and software
- Remind employees never to click on links or attachments they are not expecting
- If you need to open an attachment, save it first and then scan it with your updated antivirus and antimalware software before opening it
- Scan URLs through IT-approved websites that check URLs for blacklisting and malware
- Manage and monitor DNS as a first line of defense

In the United Kingdom, for example, a smishing campaign promising a COVID-19 financial relief payment from the government actually sent respondents to a fake government U.K. website that requested credit and debit card details. Another smishing campaign in the U.K. targeted parents with a promise of help in getting free school meals for children, but actually was an attempt to steal banking details and defraud the parents.

In the U.S., CISA, the Treasury Department, Internal Revenue Service and the U.S. Secret Service released a joint alert in May to help Americans avoid pandemic-related scams, including those designed to steal payments and personal financial data and disrupt government payment efforts.

A joint advisory group from U.S. and U.K. security agencies also was formed to protect the intelligence communities from becoming victims of attacks, particularly from advanced persistent threats from groups targeting individuals and organizations with malware. One such scam targeted the World Health Organization, where the cyberattacks were offering to provide masks and thermometers to fight the pandemic but actually were seeking confidential WHO data.

SOLUTIONS

What can local, state and federal government agencies do to defend themselves against such attacks? By far the best advice for corporate America also will work for governmental organizations. While public and private sectors have some differences when it comes to issues such as disclosure and confidentiality, the basis is the same.

At the core is user education. Helping government employees understand good cybersecurity hygiene is essential.

At the core is user education. Helping government employees understand good cybersecurity hygiene is essential. With the vast majority of office-based government employees working at home, agencies need to focus on the basics of identity management; implementing zero trust in order to protect networks from untrusted users, devices, applications and network connections; and ensuring that data is protected from unauthorized egress and access.

For those governmental agencies without existing threat intelligence capabilities, now would be a good time to invest in a comprehensive program that includes a mix of traditional data feeds, specialized feeds focusing on specific requirements for a given agency, an open source intelligence (OSINT) feed and greater emphasis on understanding the threat intel an agency already is generating from its existing SIEM systems and related log systems.

Government agencies also should take advantage of several emerging technologies to further enhance their existing security policies. For example, security orchestration, automation and response (SOAR) enhances the speed and reliability of existing operations. For cloud-based operations, a cloud access security broker (CASB) is on-premises or cloud-based security policy enforcement placed between cloud server consumers and providers. It interjects enterprise security policies as cloud-based assets are accessed.

As a key target of bad actors and nation-state cyberattackers, continuous monitoring is essential; any lapse can let attackers have access to a system, even if just momentarily.

Continuous management and monitoring adds another dimension to protecting government networks. As a key target of bad actors and nation-state cyberattackers, continuous monitoring is essential; any lapse can let attackers have access to a system, even if just momentarily.

So, how can government agencies protect themselves and their employees from potential losses? Generally, the best practices for corporations apply to government agencies as well. The foundation of cybersecurity is an educated workforce. It does not matter if the workers are on-prem or remote; if they know not to click unexpected links and images, the battle is half-way won.

CONCLUSIONS AND RECOMMENDATIONS

Governments at all levels are facing the same challenges as private-sector enterprises — the pandemic is forcing a digital transformation that puts more pressure on the government to move operations to the cloud, sometimes without having the time to do the same level of due diligence they normally would. This means governments, like their commercial counterparts, are doing all they can to either make do with the cloud resources they have or relocate their cloud business to operations that more fully align with their respective compliance and operational needs.

Governments also are trying to balance the need to move employees to telecommuting status while keeping up with both the same quality of service and meeting all of the various states' privacy and other compliance laws.

Unlike private enterprises that have the flexibility to move funds around from one account to another relatively quickly to meet specific needs, that is not always the case in the public sector. Sometimes moving funds from one department to another requires a vote of a council or legislature, and sometimes the efforts end up getting bound up in political debate that has little to do with cybersecurity.

One security professional cited "the continued threat of third-party states accessing our information as we continue to support work from home for our employees" as one of their key concerns. Another said they were worried that "currently our security systems are outdated" while another wanted to "just make sure all data is secured from all government contracts to make sure it does not leak out to the public." Still another took a more pragmatic approach, noting their "concerns about their cloud suppliers' security."

Sometimes security pros end up with conflicting recommendations based on their own experiences. For example, more than one government security pro made, in effect, the same suggestion: “By investing in the latest equipment to prevent breaches from these threats, an organization should buy the latest software and anti-theft programs.” However, another came at it from exactly the opposite perspective: “Sometimes, newer isn’t always better. The aging infrastructure while outdated and slower is more difficult to hack.”

Clearly there is no one single issue that addresses all of the challenges government security pros face. Whether the cybersecurity executives are worried about nation-state attacks, hardware configurations and capabilities, privacy, the pandemic and its own varied issues or some other worry, the same basic rules apply. In order to be safe, governments, as well as private enterprises, need to have good cybersecurity hygiene and train their employees to identify and respond appropriately to spam and other potential email-borne threats and recognize the difference between a phishing threat and a benign email.

Cybersecurity Guidelines for Government 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 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 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 294 senior-level federal, state and local government IT executives. 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. The survey also addressed questions about financial losses and network business continuity issues.

Qualified respondents were screened for being employed in an IT function at a local, state or federal government organization across a variety of agencies, including healthcare/medical, military/defense, transportation, education, court/judicial and transportation. Most of the respondents (83%) described themselves as either significant or final decision makers of cybersecurity budgets or operations.

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 8,000 customers, including 350 of the Fortune 500.

Learn more at www.infoblox.com

CyberRisk Alliance
Business Intelligence Resources

Infoblox®
NEXT LEVEL NETWORKING