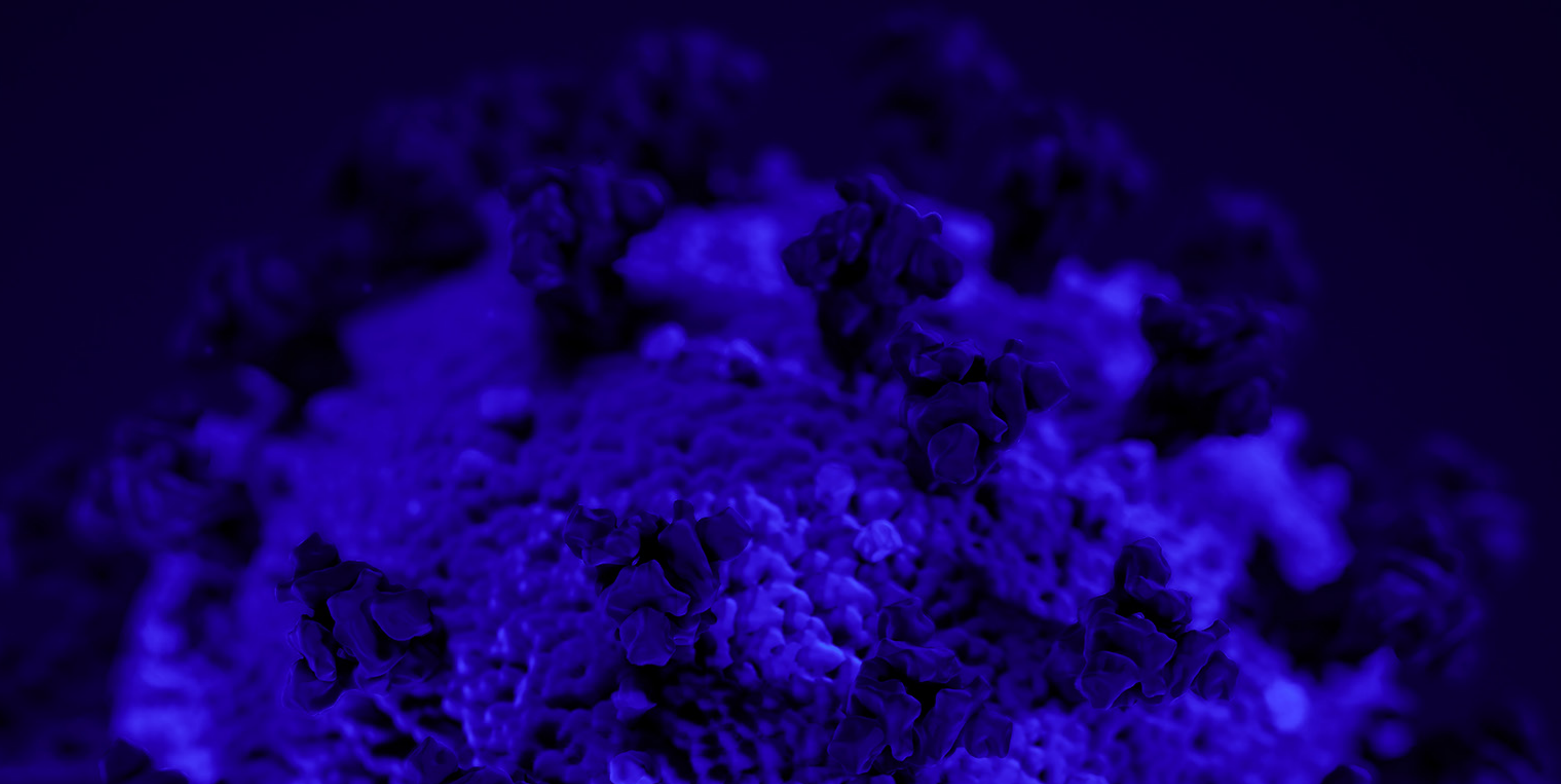
Secureworks®

Pandemic-Driven Change: The Effect of COVID-19 on Incident Response

Secureworks incident responders share lessons from incident engagements during the pandemic with advice for avoiding common issues.



A Letter From Our Chief Threat Intelligence Officer

The COVID-19 pandemic has had a global impact on lives and businesses. Expanded use of video conferencing and online services has enabled remote workforces to continue operations. However, the need to quickly respond and adapt to the situation may have caused some organizations to overlook security implications. Network defenders likely have less understanding and visibility of their environments due to continual changes this year. As organizations settle into new routines and reassess their priorities, they should conduct risk assessments to evaluate their technology investments and overall security posture. By understanding risk, organizations can identify architecture issues, gaps in security controls, areas for possible consolidation, and ways to improve their resiliency.

We have detailed in this report what our incident responders and researchers have observed in this year of change. I hope you find this report outlining what we have seen this year useful.

Barry R. Hensley

Barry Hensley
Secureworks Chief Threat Intelligence Officer

Table of Contents

Introduction

The COVID-19 pandemic changed the way the world works, with organizations shifting to home-office work styles literally overnight. In fact, the Secureworks incident response team found that most organizations closed their physical work environments to move to remote work—often overlooking security controls for the sake of "just getting things done." Meanwhile, some IT and security departments experienced workforce reductions which made security operations and incident response harder. While cybersecurity professionals were in high demand, tough financial and economic conditions created uncertainty. Many threat actors used COVID-19 as an opportunity to employ familiar tactics such as phishing, using the pandemic as bait. Secureworks observed government-sponsored hackers weaponizing COVID-19-themed Microsoft Office documents.[1]

Initial news reports suggested a sharp uptick in cyber threats after the pandemic took hold. However, several months into the pandemic, Secureworks data on confirmed security incidents and genuine threats to customers showed the threat level largely unchanged from before the pandemic. Instead, major changes in organizational and IT infrastructure created new vulnerabilities which threat actors sought to exploit. The global nature of the pandemic also saw the targeting of healthcare, pharmaceutical, and government organizations by both nation-states and financially motivated cybercriminals. Nation-state actors were particularly interested in information related to vaccine development and pandemic response strategies.[2] Cybercriminals of all kinds recognized the large sums of money funding pandemic-related work and targeted the data for financial gain.

Infrastructure transformed practically overnight for many organizations. A sudden switch to remote work, increased use of cloud services, and increased reliance on personal devices created a significantly expanded attack surface for many enterprises. Facing an urgent need for business continuity, most companies did not have time to put all the necessary protocols, processes, and controls in place.

These factors made it difficult for security teams to respond to incidents. Gaps in security controls, logging, and visibility were common as security and IT teams moved fast to enable business, foregoing the necessary security architecture review out of expediency. This made it harder for incident responders to build a complete picture of events. Some organizations did not anticipate the need for remote access to certain critical assets and struggled to provide access to them. Use of personal computers in some organizations complicated the legal landscape around remote access for incident investigation. Secureworks incident responders also worked with IT and security teams that had experienced furloughs and layoffs due to the economic impacts of COVID-19.

Secureworks incident responders helped organizations navigate the challenges of the pandemic to prevent, detect, and respond to a wide range of cybersecurity incidents. This report shares the observations of Secureworks incident responders about how COVID-19 changed the state of cybersecurity posture for organizations. It also analyzes the major incident response challenges Secureworks incident responders dealt with in the field and offers advice to help you avoid the same mistakes.

The State of Cybersecurity Risk

When the COVID-19 crisis struck, organizations had to quickly shift to remote work—without the time to analyze, design, and implement necessary security controls. Cloud transition projects were accelerated, and many security teams did not have time to properly assess the new services or deploy controls such as multi-factor authentication (MFA). Due to the pandemic, adversaries targeted healthcare, pharmaceutical, and government organizations for their intellectual property. The Secureworks incident response team engaged with a large number of enterprises during the pandemic. They saw the changed risk landscape manifest in the following ways.

Increased Risk From Remote Workforces

The rapid shift to work-from-home environments put immense stress on existing cybersecurity controls and operations. Many organizations simply had not designed their networks for a totally remote workforce and did not have the right bandwidth or network monitoring tools in place. Secureworks incident responders saw customers experiencing increased risk in these areas:

Lack of Multi-Factor Authentication (MFA) — Social engineering ploys and other types of credential theft keep occurring, making MFA increasingly important. Yet, organizations were reluctant to deploy MFA because of the potential for disrupting remote workers by slowing down the roll-out of remote services. The urgency of providing remote access to unexpectedly large numbers of staff may also have meant that MFA was delayed as a security enhancement that could be added later, but never was.

Access to SaaS Applications — To get around corporate VPN bandwidth limitations, organizations allowed remote users to access SaaS applications on devices directly, rather than through the VPN. This bypassed security controls and impeded visibility and logging, putting sensitive data at risk.

VPN Split Tunneling — To alleviate the strain on undersized VPN solutions, organizations used split tunneling to route some traffic through the encrypted VPN tunnel, while allowing other devices or applications to access the internet directly. This meant reduced visibility as incident responders had limited access to log data outside of VPN traffic. In one incident, this split tunneling configuration meant that malware command and control traffic from an infected host went directly out to the internet, rather than through a monitored egress point, and the initial compromise was missed. The dependency of remote workers on these access solutions also meant some containment and eviction activities had to be delayed to ensure they would not adversely affect users.

Security Monitoring and Access Control Implications — Many security appliances, VPN concentrators, firewalls, and proxies were undersized for remote workforces. This may result in performance and usability issues, and also lead users to seek alternatives with less control and visibility in order to complete their work.

Delays in Security Patching — For many organizations, operational priorities delayed patching of internet-facing systems and remote access services, even when those systems were most at risk. This meant that even where organizations had deployed MFA, adversaries were able to bypass it by using publicly available exploit code to compromise the underlying software and hardware.

Personal devices were another critical concern. Many organizations did not have the hardware to support an entirely remote workforce, so they allowed personal devices to be used instead. It was at the opposite end of the spectrum from a carefully deployed Bring Your Own Device (BYOD) policy with strong endpoint protection and perimeter access controls. If these personal devices are involved with a security incident, responders are faced with both logistical and legal challenges. Does the organization have the legal right to examine the device? Can they physically get access to it?

Secureworks also observed that organizations accelerated their transitions to cloud-based collaboration services, such as Microsoft Office 365 (Microsoft 365). Many cloud services are equipped with robust security features, but these require configuration by an organization to suit their own needs. Under the pace of change during the pandemic, the necessary due diligence did not always occur. As a result, monitoring and control capabilities that previously existed were eliminated, creating dangerous security gaps.

The FBI also warned of teleconferencing services being hijacked by opportunists inserting lewd or offensive material into the session.[3] This practice, also known as Zoom bombing, did not require significant technical skills, and was likely often perpetrated by non-technical users in a manner closely resembling internet trolling, rather than traditional cybercrime. It mostly caused disruption and a lack of confidence in the conferencing solutions. Secureworks incident responders did not encounter any serious security incidents that were the result of Zoom bombing.

Areas of Increased Risk From Personal Devices

Secureworks incident responders identified some key issues with the increased use of personal (third-party) devices for remote work. If your organization is using third-party devices to perform work, it is harder to protect organizational data from compromise or exposure.

Some potential issues include:

- Lack of monitoring/visibility for protecting against threats
- Systems are not locked down
  - unencrypted data at rest
  - weak or no passwords
  - users have local admin rights
  - USB ports are enabled
  - patches may not be up to date
  - other configuration vulnerabilities
- Limited employee awareness of risk-mitigating behaviors
- Potential legal issues with responding to incidents
- Inability of security teams to access devices remotely or isolate them completely

Mitigation of these issues takes a combination of policy, technical controls, and employee education. It is important to work with legal counsel to ensure there are necessary policies and agreements for employees related to allowing potentially sensitive company information to be stored and processed on a third-party device. Once these are established, to the extent possible the company should establish technical controls to help monitor and enforce these policies. For example, provide configuration profiles to enforce data encryption and password strength, or install technical controls such as a Mobile Device Management (MDM) solution.

It is also important to work with legal counsel to develop incident response processes where third-party owned devices are involved (such as authorization to conduct analysis on such a device).

Increased Risk From Staffing Changes

The COVID-19 pandemic has caused a dramatic and negative business impact. The ripple effect included shrinking IT budgets and shifting cybersecurity priorities. As a result, many organizations were suddenly forced to downsize their workforces. Nonetheless, business technology still required the same – and oftentimes more – IT security and support services as they did pre-COVID-19. Reduced workforces still had to implement basic IT security measures such as patch management, detecting malicious activities, or simply providing timely desktop support. In addition, IT professionals were also responsible for ensuring that the massive shift to work-from-home and remote access technologies remained secure for its employees and supply chain partners.

Incident response teams also operated remotely during the pandemic. At Secureworks, this did not represent a significant shift in work processes from pre-pandemic circumstances. At the beginning of March 2020, roughly 50% of Secureworks employees worked remotely on a regular basis. The shift to full remote work was smooth for the incident response team and backed by already existing security measures that enabled a remote workforce globally. Though Secureworks incident responders already had capability to fully support customer incidents through remote work, they still faced new challenges caused by changes in customer operations and environments. Compromised systems were now sitting at employees' homes, rather than in an office. In some cases, the computer was still in the office, but security teams could not physically get to it. Lockdowns restricted employee access to buildings and use of personal devices created legal gray areas around access by both the employer and the Secureworks incident response team.

Increased Risk for Healthcare Sector

Organizations directly involved with the public health crisis, including government, healthcare, and pharmaceutical organizations, were also at greater risk of attacks related to the pandemic. Government-sponsored threat actors increasingly targeted research facilities to acquire or manipulate sensitive information, including COVID-19 vaccine and treatment research.

> **At the beginning of March 2020, roughly 50% of Secureworks employees worked remotely on a regular basis.**

REAL-WORLD EXAMPLE

Termination of Remote Employee With Privileged Access

Secureworks incident responders worked with an organization that had to terminate an employee with privileged access credentials over the phone due to a COVID-19 office shutdown. Prior to the pandemic, employees at the organization would physically return laptops or workstations. After receiving the computers, the IT team would eventually disable credentials. Risk was lower as the former employees no longer had access to the devices. However, because this privileged employee was now working remotely, they delayed sending devices back to the office. As a result, Secureworks incident responders observed this employee using the company device to access assets after termination. The former employee had multiple accounts with elevated access, which made the incident harder to remediate.

A Familiar Threat Landscape

Throughout the pandemic, threat actors shifted tactics to take advantage of heightened concern and interest in COVID-19. While initial media reports seemed to suggest a sharp increase in the number of threats, Secureworks researchers observed no significant change in overall threat volume. Adversaries simply pivoted their tactics to launch COVID-19-themed campaigns, exploit the security gaps in remote work environments, and target organizations involved with pandemic research.

COVID-19 as Phishing Bait

Cybercriminals and government-sponsored threat groups exploited fear and uncertainty around COVID-19 to lure users into clicking on malicious links and opening malware-laden attachments. Threat actors exploited uncertainty and the desire for information by masquerading as trusted entities to gain initial access to their targets, commonly using email and SMS. The activity prompted joint alerts from US and UK cybersecurity agencies.[5]

Some examples of the phishing campaigns include:

COVID-19 stimulus check fraud, where threat actors used phishing pages disguised as Internal Revenue Service tax forms to steal identities and apply for a victim's stimulus relief check.[6]

COVID-19-themed phishing emails with malicious Microsoft Excel attachments, which triggered the download of information-stealing malware (also known as an infostealer).[5]

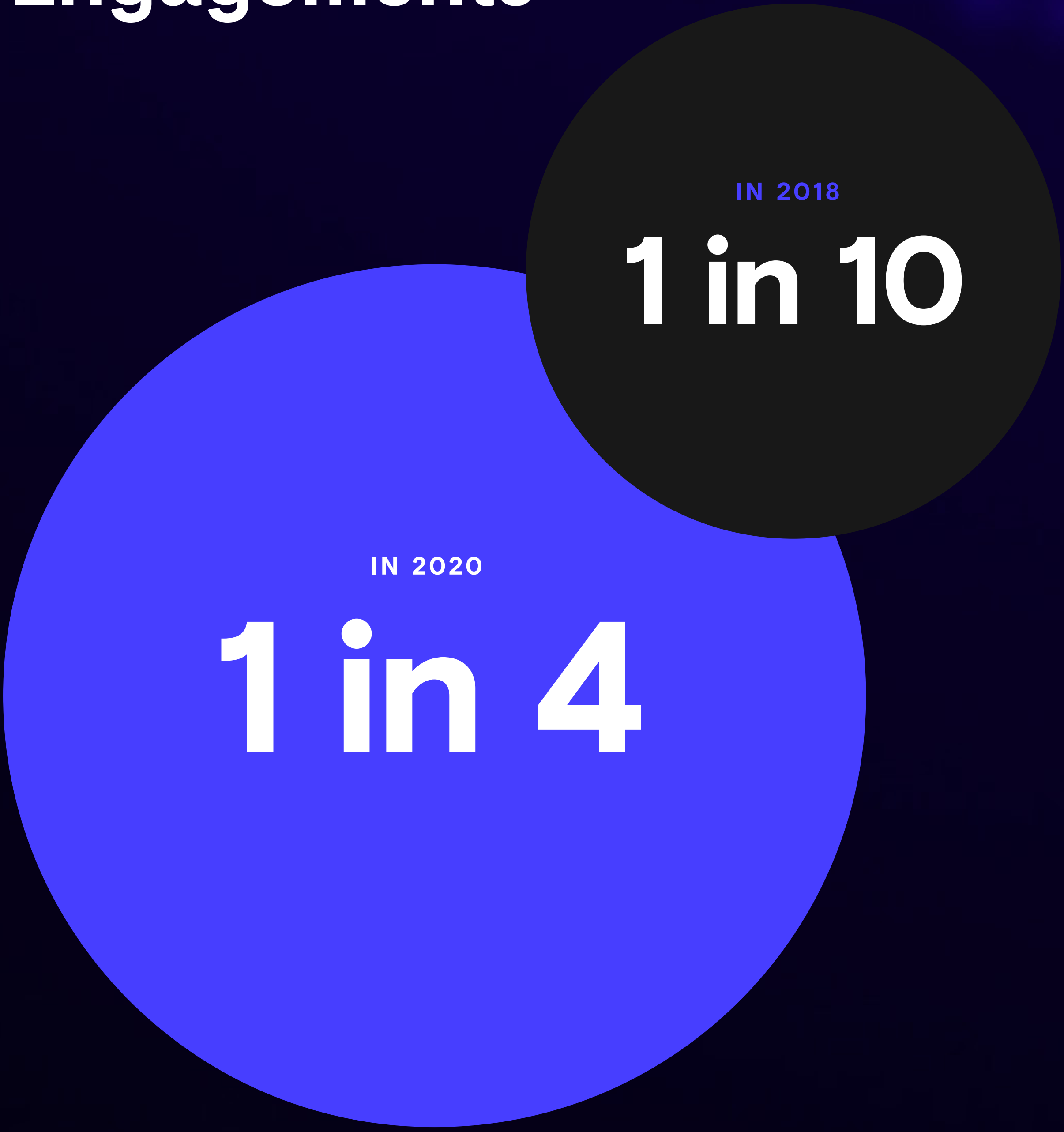
Multiple phishing emails tried to steal user credentials using **spoofed login pages** with COVID-19-related wording (such as "COVID-19 advisory").[5]

A series of SMS messages used a UK government-themed lure to harvest banking information.[5]

Phishing emails that appeared to come from the World Health Organization (WHO) **delivered the LokiBot infostealer.**[1]

One email with tips on how to avoid COVID-19 scams actually delivered a **banking trojan.**[1]

Secureworks Ransomware-related Incident Response Engagements



IN 2018

1 in 10

IN 2020

1 in 4

Credentials Abuse During the Pandemic

Secureworks incident responders helped several organizations respond to incidents of unauthorized credentials-based access. Social engineering attacks had a greater chance of success with remote workers, who could be tricked into releasing their credentials over the phone, by text, or in chat applications. Threat actors were also able to purchase data packages from underground forums, giving them access to stolen personally identifiable information which simplified the tax identity theft process.[6]

Secureworks researchers have observed cybercriminals discussing the success of COVID-19 fraud attempts and soliciting partners to share resources.[6] In one example, a threat actor with knowledge of banking terms of service, and who had access to full credit information, sought help from somebody who knew of creative ways to cash out fraudulently acquired pandemic stimulus checks.

Using MFA for internet-facing resources, encrypting your sensitive data, and disposing of information securely remain vital best practices to protect against credentials abuse.

Network Scanning and Exploits

As mentioned earlier, Secureworks telemetry shows that there has been no overall upturn in intrusion activity or in confirmed security incidents during the pandemic. However, threat actors did increase their scanning of networks for remote access service vulnerabilities—from unpatched VPNs to new deployments of cloud applications.

THREAT TACTICS:

If It Ain't Broke, Don't Fix It

Threat activity during the COVID-19 crisis has looked about the same as pre-pandemic. Most of the observed attacks were financially motivated, although the FBI also warned about nation-states targeting organizations involved with COVID-19 research.[3] Observed threat tactics have included:

Ransomware

Ransomware continues to be a scourge on organizations. In 2018, 1 in 10 Secureworks incident response engagements were ransomware-related. In 2020, that proportion has increased to around 1 in 4. Toward the end of 2019, criminals escalated the impact when they realized they could gain additional leverage by stealing data before encrypting it and then threatening the victim with public disclosure.[4]

Downloaders/Modular Malware

Malware families, such as Emotet and TrickBot, are able to download additional payloads, steal credentials and other data, spread programmatically to compromise other hosts across the network, and can be an enabler for disruptive ransomware attacks.

Business Email Fraud

Email accounts are compromised, both those hosted locally and in cloud services like Microsoft 365, and colleagues are targeted to transfer money to threat actor accounts.

Insider Threats

Employees with administrator privileges can install unauthorized tools, tamper with systems, and access all kinds of sensitive information.

REAL-WORLD EXAMPLE

Network Security Threats

Secureworks incident responders worked with an organization that had provided desktop PCs for employees working remotely. But the PCs were configured with remote desktop protocol (RDP) enabled—and when an employee plugged the PC directly into an internet modem (with no firewall or other protection in place), the system was left wide open. A threat actor launched a brute-force attack via RDP and obtained credentials.

Fortunately, a cloud-based endpoint detection and response (EDR) tool detected the incident and Secureworks helped mitigate the threat before any damage occurred. This illustrates why organizations should understand the authorized use cases for employees and configure systems accordingly. Organizations should also clearly document and train remote workers on proper system use.

Incident Response During the Pandemic

The foundation to effective incident response applies no matter the circumstances: people, processes, and technologies aligned with security as a core focus. When it comes to the COVID-19 pandemic, incident response processes should account for a distributed response team that needs to mitigate issues remotely. For example: disabling a remote device, imaging a remote device, and communicating with remote employees.

People

Adversaries exploit natural and man-made disasters to target people's emotions. Fear, sympathy, and anger are often heightened in these situations, and the COVID-19 pandemic is no exception. Educate employees at every level about the heightened risk of COVID-19-themed phishing attacks, show them how to identify potential phishing, and tell them where to go with any security concerns (phishing, social engineering, and otherwise). In addition, organizations should regularly update employees on pandemic-related topics and offer straightforward guidance about how to stay secure while working from home.

Secureworks incident responders observed service desk personnel struggling with their new remote status on multiple occasions. These employees sometimes lacked the awareness to identify genuine security threats among the IT queries they processed. To help expand their security awareness, you should train IT staff on fundamental aspects of information security awareness, and their role in helping to identify, contain, and escalate potential information security issues.

The basic training could include:

- Awareness of precursors of potential malware or other information security issues.
- Asking important questions if there is concern that the issue is malware related.
- What not to do if malware is suspected – such as remoting into the machine with admin privileges.
- Actions users can take to help prevent spread of malware – such as disconnecting from network.
- Know the documented escalation path to take if dealing with a potentially serious security issue. For example, immediate notification to supervisor or CSIRT, if that path exists.

Processes

The COVID-19 pandemic revealed that many organizations had gaps within their disaster recovery plans (DRP) and business continuity plans (BCP). In most cases, these plans had not addressed a situation where all facilities would close and most employees, contractors, and vendors would switch to remote work. This caused organizations to scramble to transition their IT infrastructure to accommodate a distributed and remote workforce.

Secureworks incident responders worked with organizations to review their DRPs and BCPs, identifying ways to update the plans with input from their IT, security, and related subject-matter experts. It is critical for your organization's leadership to know what's covered in DRPs and BCPs. The pandemic also emphasized the need to revisit the plans on a yearly basis, at a minimum.

What about the operational processes for security teams? Cybersecurity incident response plans, security playbooks, and related policies need to align with how business circumstances changed.

Some questions to consider as you review these processes within your own organization:

- How do incident responders collect evidence (memory, disk images, and so on) when computers are geographically dispersed? What are the implications when personal devices are used? You should work with your legal advisors to arrange protocols for collecting data from personally owned devices during an incident.
- How are tools pushed to remote systems? Many organizations rely on technology that needs to be connected to a central network.
- How do security teams "re-image" a remote device?
- How should response teams (both core and extended teams) work together remotely?
  - How do they securely communicate?

Finally, organizations must define their processes for commanding incidents remotely. There must be a clear process for the incident commander to interact with stakeholders to make key decisions. Does your organization have someone internally that can lead an incident or is an external resource needed?

Detection and Response

Monitoring technology, such as EDR tools, are essential for detecting security incidents before they result in operational risk. Organizations need visibility across today's disjointed networks, where it is difficult to guard against both vertical and horizontal attacks. The telemetry needs to include all endpoints—not just critical services—as you need broad visibility across the infrastructure to see where an adversary is and what they are doing. Other detection and response technologies that cover network and cloud activity should also be considered to enable better event correlation and provide a complete picture of your environment. You also need the capability to support each phase of incident response remotely, from identification and containment, to eradication and recovery. Additionally, organizations need to conduct a security assessment to guide on the deployment of the right architecture and tools to protect critical data.

The COVID-19 pandemic highlighted that technology changes can impact user behavior. New tools and processes may expose vulnerabilities if areas are not locked down and users are not properly trained (such as with Zoom, VPNs, and cloud services).

At the same time, cybersecurity teams contended with their own technology changes. Many organizations rapidly transformed their IT infrastructure to support fully remote work, and evolved IT security alerts and logging in the process. Security teams increased their remote monitoring of collaboration tools, network access (via RDP or VPNs), and employees and endpoints. Logging strategies needed changing to ensure proper visibility across changed infrastructures.

REAL-WORLD EXAMPLE

Remote Incident Forensics

The Secureworks incident response team worked with an organization that had deployed new laptops to remote employees—but no EDR software had been installed before a Ransomware incident occurred. Even after deploying an EDR tool, responders were unable to reach the compromised systems. They also did not have a process for performing forensics remotely. It took days to remediate the remote endpoints. One endpoint, which was actively running malware, took weeks to remediate. The result? A different threat group almost successfully deployed a Ransomware attack in the middle of recovery efforts from the first incident.

Top 10 Ways to Improve Your Incident Response

The challenges of the COVID-19 pandemic offered organizations an opportunity to reimagine incident response plans and prepare for future unknowns. The following recommendations are intended to help you protect your organization and build dynamic incident response readiness to meet future challenges. These recommendations come straight from Secureworks incident responders who have helped organizations worldwide prevent, detect, and respond to threats during the pandemic. Remember to prioritize any changes within your existing cybersecurity framework—whether it is from the National Institute of Standards and Technology (NIST) or another framework. Incorporate pandemic scenarios into your resilience assessment.

1

Use MFA for All Access Possible, Especially Remote

Use MFA for all possible services, but at a minimum, all remote services, including cloud applications such as Microsoft 365 and external VPNs. Users must provide a second factor in addition to their regular password. Avoid using email or SMS text messages as a second factor as threat actors can intercept these methods. And remember: MFA is essential, but only one component of a security strategy.[7]

2

Gain Visibility With EDR Tools

Deploy EDR tools to detect suspicious activity that other controls have missed. Use cloud-based EDR tools to capture data on the endpoints, rather than relying solely on firewalls, proxies, or netflow connectors. This means that wherever the end user goes, the data is collected and available for investigation and forensics.

3

Plan for Remote Incident Response

Define processes and personnel to collect forensic data remotely, and coordinate incident response activities without too much dependency on key individuals. For example, you should define emergency procedures that give others access to key systems, and establish a network “kill switch” that shuts down specific services while allowing remote administration. This way, you can turn off OneDrive synchronization, disable VPN access, and notify users to effectively contain incidents.

4

Develop Baseline Configurations

Refer to expert sources such as the Center for Internet Security[8] and the National Security Agency[9] for recommended security configurations for a wide range of operating systems and applications. Hardening typically involves removal of unnecessary accounts, disabling/removal of unnecessary services, and enabling of security-conscious configurations. Consistently manage systems, proactively deploy patches, and regularly scan to detect and remediate vulnerabilities.

5

Secure Remote Access

Reduce risk by requiring remote workers to use organization-provided VPNs, DNS servers, and web filtering/reverse proxy solutions for secure remote access. This will provide a more secure environment for your workforce and more actionable information for incident response.

6

Update BYOD Policies

Evaluate your information security policies and analyze whether they meet your security objectives. Consider training remote workers on home office security, social engineering scams, physical security of critical IT assets, proper VPN use, and the use of mobile Wi-Fi for connectivity, where appropriate.

7

Strengthen Remote Termination Processes

Fine-tune your termination processes for a fully remote workforce. Schedule a day and time to disable a terminated employee’s access to IT resources, including their email account and social media profiles. Proactively manage privileged account credentials and remove any unrecognized accounts.

8

Revise Remote Help Desk Processes

Beware of social engineering attacks on the help desk, which can be more difficult to monitor with a remote workforce. Consider verifying the legitimacy of requests for sensitive data or account updates by using previously established offline channels, such as the telephone. Expand “First Alerter” training to help staff quickly identify potential security issues to escalate and contain them.

9

Plan for a Secure Transition to Cloud Services

Maintain strong access control across your cloud services (such as MFA), ensure that you can detect any intrusion attempts, and update your incident response processes to account for remediating threats within the cloud environment.

10

Scale Capacity for Remote Connectivity

Expand your VPN capacity to allow for more remote workers to securely access your resources. Or, if you have VPN limitations, consider using other remote access solutions to provide secure access to your environment, such as virtual desktop infrastructure.

Conclusion

The pandemic has changed the way the world works, but cybersecurity threats are largely the same. Threat actors continue to use malware, phishing, and other social engineering tactics to take advantage of victims for their own gain. Organizations can bolster their defenses by training personnel and tuning their processes and tools for work-from-home environments. This can help organizations better prepare to detect and respond to incidents well into the future.

Secureworks experts can help your internal teams reduce risk with a team backed by years of experience with incident response and threat remediation. Learn how to minimize the impact and duration of cyber incidents, empower your staff against emerging threats with proactive incident response plans, and mature your incident response program with a proactive approach.

Secureworks®

About Secureworks Incident Response

The Secureworks incident response team provides a wide range of expertise, cyber threat intelligence, and purpose-built technologies to help organizations prepare for and respond to cyber incidents successfully. Secureworks can assist organizations with onsite (subject to applicable pandemic travel restrictions) or remote Incident Commanders in support of an incident response. Secureworks experts work closely with in-house teams via emergency incident response services, threat hunting assessments, tabletop exercises, and a range of other incident readiness services – all designed to help you build an incident response program and resolve incidents efficiently and effectively at scale.

About Secureworks

Secureworks® (NASDAQ: SCWX) a global cybersecurity leader, enables our customers and partners to outpace and outmaneuver adversaries with more precision, so they can rapidly adapt and respond to market forces to meet their business needs. With a unique combination of cloud-native, SaaS security platform and intelligence-driven security solutions, informed by 20+ years of threat intelligence and research, no other security platform is grounded and informed with this much real-world experience.

www.secureworks.com

Sources

[1] Secureworks Counter Threat Unit™ Research Team, "How Cyber Adversaries are Adapting to Exploit the Global Pandemic," Secureworks blog, April 8, 2020.

[2] Secureworks, "Don't Wait for Them to Find You: What You Need to Know Today About Nation-State Threat Actors," Secureworks blog, August 25, 2020.

[3] FBI, "Criminals and Nation-State Cyber Actors Conducting Widespread Pursuit of US Biological and COVID-19 Related Research," FBI Private Industry Notification, May 21, 2020.

[4] Secureworks Counter Threat Unit Research Team, "Preparing for Post-Intrusion Ransomware," Secureworks blog, June 29, 2020.

[5] US Cybersecurity and Infrastructure Security Agency Alert, "COVID-19 Exploited by Malicious Cyber Actors," April 8, 2020.

[6] Secureworks Counter Threat Unit Research Team, "Cybercriminals Target U.S. Citizens for COVID-19 Stimulus Fraud," Secureworks blog, May 6, 2020.

[7] Secureworks Adversary Group, "Think MFA is Hack-Proof? Think Again," Secureworks blog, April 30, 2020.

[8] Center for Internet Security, CIS Benchmarks

[9] National Security Agency, Security Configuration Guidance