CEP Magazine - January 2021

Protecting corporate data in the work-from-home era

By Melody Haase

Melody Haase (melody@4discovery.com) is the Head of Client Success at 4Discovery, a digital forensics firm based in Chicago.

- linkedin.com/in/melodyannhaase/

Work restrictions created by COVID-19 forced companies worldwide to quickly adopt technologies and fundamentally change the way they do business. In October 2020, McKinsey & Company released the results of a survey that showed companies exponentially adopted digital technologies to do business, and these same companies do not expect that to change.[1] However, in a rush to adopt new technologies during a crisis, companies were often focused on business continuity rather than security.

Security companies around the globe have reported increases in ransomware, data breaches via email, and unauthorized access of systems. Data breaches of all shapes and sizes can fundamentally impact a company's ability to do business and/or its reputation. Many articles about data security are focused on outrageous statistics and horror stories of businesses shutting their doors because of a security incident. Rather than focusing on scary statistics and costly solutions, this article will focus on general security concepts and some common things companies can do to enhance corporate data privacy during the work-from-home era. By the end of this article, readers will be better informed and more prepared to take the next steps to protect corporate data.

Understanding the threat landscape

Security threats can largely be placed into two categories: internal threats and external threats. Internal threats typically arise because of some sort of employee behavior, whether intentional or not. This can take many forms, such as an employee who becomes the victim of a phishing attack, a rogue employee who steals data, or an employee who carelessly leaves sensitive files in an unsecured location. External threats are actors outside of the organization that are aimed at gaining access to corporate systems and data. Typically, they gain access to systems by leveraging poor security practices, malware, or exploits. Luckily, many of the tools used to thwart bad actors can be used to mitigate both internal and external threats.

Additionally, every company has different clients, employee bases, and thresholds for risk tolerance. This can affect how each company views security. There is an age-old debate in the security industry about security vs. convenience. For those promoting security, there is a push for more protections and steps to access systems. For those who promote convenience, there is a push for less security to make systems easier to access for the sake of business convenience. However, there are always implications to these decisions that may require companies to change the way they do business.

A great example of how to think about security vs. convenience is using the practice of blacklisting IP addresses by country. Blacklisting is the process of blocking items. In this context of IP addresses, it means that you can choose to block all IP addresses coming into your systems from hacking hotspots like Russia or China. If a company only does business inside of the United States and only has employees inside of the United States, it may be a feasible option to turn off the rest of the world's IP address range. However, it may be more complicated and less feasible for a global business to employ these same policies to reduce risk because it may affect its ability to provide system access to its customers and employees.

Physical security has drastically changed

Before COVID-19, companies were accustomed to all of the physical and environmental security in their facilities. Security cameras were online to monitor physical activities inside of locations. Badge access was required to enter buildings. Shredding boxes were placed around locations to ensure sensitive data was disposed of properly. Printers asked for passwords before printing to prevent the wrong person from picking up sensitive documents. Locked file cabinets were housed in offices to prevent access to sensitive files. Doors were placed on offices and conference rooms to prevent people from hearing confidential phone calls.

Work from home has completely upended the physical security environment. When COVID-19 hit, many individuals were not prepared to work from home. Many people did not even have workstations or desks. Many homes do not have security cameras or require badge access. Shredding, printers with password access, and locked file cabinets are likely not available. Spouses often share workspaces and hear each other’s conversations. If the company is allowing Bring Your Own Device (BYOD), it also means that the computer being used for work may or may not have shared access between numerous individuals in the house. While companies may not be able to control this environment, they can, at a minimum, provide training to employees, as well as provide them with more secure ways to access systems.

Security requires a shift in mindset

In order for companies to transition traditional security practices to work from home, more emphasis must be placed on giving employees tools to be successful with their personal security, including training them on basic security practices. Many corporate security exercises contain information about and examples explaining what to do inside of an office and the corporate environment. However, this training typically does not include information on keeping data secure in an unsecured environment like a typical home setting.

Training should be changed to focus on the employee’s home security practices and how they relate to corporate data security. Some items employees should be educated on are:

- Changing standard settings on routers and modems;
- Checking and strengthening security settings on their operating systems, web browsers, and other applications;
- Limiting the number of applications they install to prevent application-level security issues;
- Creating unique usernames and passwords for devices and accounts that house corporate data;
- Spotting phishing and malware attack threats that they may encounter;
- Protecting physical access to devices containing corporate data;
- Disposing of documents in line with corporate policies; and
- Reporting security incidents to the appropriate parties.

Employees should be reminded of security often. They must be reminded that they are constantly interacting with confidential corporate data and should act accordingly. If the company has a corporate newsletter or bulletin, dedicating a portion of it to security practices can be extremely beneficial. It can help reinforce the items learned during training as well as provide employees updates about changes in the corporate security environment.

A primer on BYOD

At the beginning of COVID-19, many employees that typically worked in secure corporate environments were sent home to work on home computers, personal cell phones, and home networks. From a security standpoint, BYOD is not recommended. It is a great area of risk, and policies and practices related to BYOD are riddled with issues. There are simply too many variations on BYOD for an in-depth analysis in this article. However, because of BYOD's risk, it is necessary to stop and consider it as part of a general security plan.

These personal devices often have no form of mobile device management or data loss prevention software installed on them, both of which provide an extra layer of protection to corporate data and accounts by allowing corporate information technology (IT) to have some administrative oversight of the device and the data contained on the device. When companies allow individuals to use their own devices for work without any protections, the company ultimately loses control of that device and the data stored on it.

Because the employee owns the device and controls access to the device, it becomes complicated and can even become a legal battle to perform basic functions such as protecting data for litigation holds and retrieving data for internal investigations. Similarly, employees control security patches and have the ability to install whatever software they want. This can allow insecure devices to connect to corporate infrastructure and create additional security incidents. Most importantly, employees can commingle personal and professional data on any of their devices and accounts.

Often, BYOD policies, processes, and procedures do not require employees to sign a declaration certifying they have deleted corporate data from the device and/or their personal accounts upon the termination of their employment. This declaration is beneficial to collect in the event litigation for theft of corporate data needs to occur. At a minimum, every company should stop and consider its current BYOD practices, conduct a risk assessment regarding the safety and security of the data accessed by BYOD users, check if its policy is currently updated for COVID-19-related activities, and ensure the policy addresses how to retrieve and/or certify the destruction of corporate data at the end of the work-from-home period or upon termination of employment.

Security starts at the top

While the first part of this article focused on employees and the home environment, the major component of corporate security comes from within. Corporate security is best implemented, practiced, and enforced when it comes from the highest leadership levels. Communication about security and buy-in needs to happen at all levels of the organization to ensure that all security policies and practices are followed. How do you create a culture of security?

Start by conducting an assessment of your policies and procedures. Each of them needs to be updated to adjust for employees who are now potentially working in unsecured areas using unauthorized equipment and accounts. Simultaneously, the incident response playbook should be reviewed and updated to ensure parties still have a streamlined way to respond to incidents. Once updated, these policies and procedures should be redistributed to employees for review.

This should all be pushed out with an enhanced work-from-home training program as described above. Provide employees with common examples of security mistakes, how they affect the business, and how they could have been prevented with stronger security practices. These exercises do not need to be extravagant. Simply focus on the most important areas of data security for your organization.

A cycle of continuous security improvement

A security assessment of the organization’s current technology environment needs to be conducted. Network infrastructure, individual devices, and online accounts all have potential security issues that need to be checked. At 4Discovery, most of the security incident response cases we have worked on thus far had a simple root cause, such as a security setting that was never changed when a system was implemented, a system that was unpatched, or reusing an administrator username and password throughout an entire infrastructure.

IT should constantly be in a cycle of continuous security improvement as a common course of practice. Below are some helpful practices to combat common weaknesses used by attackers to gain access to systems.

Take password protection seriously

One of the most common methods used in data breaches is password compromise. Ensure all default administrator usernames and passwords have been changed for off-the-shelf devices. Create unique administrative usernames and passwords for individual pieces of infrastructure. All accounts must require strong passwords that are long and use a variety of characters. Along those same lines, password changes should be mandatory on a routine basis to prevent any user credentials that may have appeared in past data breaches to be used to access systems.

Use multifactor authentication everywhere possible

Multifactor authentication (MFA) should be required for all accounts that have the option. MFA is the process by which a user needs at least two things to enter a system. Some commonly used forms of MFA are two-factor authentication text message codes, and hardware- or software-based tokens. While two-factor authentication text codes are not recommended as a best practice for MFA, simply having them in lieu of nothing adds an additional layer to account security.

Employ the POLP

Simply looking at all of the account settings in systems and evaluating them using the principle of least privilege (POLP) can help immensely when strengthening systems. POLP simply means that individual users only need, and thus should only have access to, the least amount of system access necessary to perform a task. Reducing people’s access to systems and data limits the ability of bad actors to move throughout corporate systems using their accounts. It also hinders rogue employees who may attempt to access and exfiltrate confidential data.

Control all programs and settings

Use gold images and control the device from the start. Gold images are the standard settings and programs that are deployed on corporate assets. By using a gold image, IT can more quickly set up new machines while customizing settings to least privileges before deployment. When creating a standard, think about how much of the internet employees need to access. Do they need the ability to install software, and are they going to need to plug in USB devices? These are all common ways people exfiltrate data and attempt to cover their tracks. You can also combine this practice with POLP role-based permissions, common data loss prevention software, and/or device management solutions to maintain more control over the devices and data.

Interrogate and harden all default settings

Many systems and applications come with minimal security settings for the sake of convenience for the average user while sacrificing some security. This is done with the expectation that the user or administrator will strengthen the settings as necessary. This can be as simple as ensuring the firewall is not speaking to the entire internet, making applications ask for camera and microphone permission, and turning on logging and monitoring. The goal is to prevent bad actors from having easy access and provide IT with the tools they need to monitor attacks.

Continuously update systems

Setting a routine software update schedule every week is crucial. As an example, WannaCry and other ransomware forms were able to spread throughout the globe because systems went without patches for over two months. Years later, many systems still had not applied the patch Microsoft issued in March of 2017.[2] If companies would have taken the proactive steps to fix their systems, the vulnerability would have been patched, and system access never would have occurred.

Encrypt traffic with a VPN

While an organization may not be able to control an employee's home router settings, it can provide a safe way for its employees to access systems. Setting up a virtual private network (VPN) to route internet traffic from the machine to its destination will help prevent attackers from accessing unencrypted data in transit. This way, in the event there is an unsecure network connected to a corporate asset, there is an extra level of data protection.

Preparing for the inevitable

The fact of the matter is that every company will suffer data loss at some point. Once an incident occurs, it is important to respond and recover from the event in a timely fashion. Aside from having an up-to-date incident response playbook, the three most important things postincident are logging, backups, and insurance.

Often, systems have settings for logging that are turned off by default. By turning on logging, analysis can be performed on system access to understand how the system and data were accessed and/or exfiltrated. Because many incidents happen months prior to the time they were noticed, archiving logs before they age and roll off in the system can provide a historical library for later analysis.

Similarly, systems have settings for backups that are not enabled by default. Turn on backups and use the 3-2-1 backup rule. Keep at least three copies of your data, in two different mediums, with at least one of them kept off-site. Backups are critical in the event of attacks like ransomware, so they should also be routinely tested to ensure they are good backups. Having recent backups minimizes data loss and provides the capability to get systems back up and running in the wake of an attack. Along the same lines, make sure to take a forensic image or remove the hard drive from the computers of departed employees to preserve historical data.

Insurance is a great tool in risk mitigation related to security incidents. Generally, there are cyberliability, cyberinsurance, and business interruption policies that may apply to these events. Each policy covers different aspects of data loss. When speaking with your insurance carrier and counsel, make sure to ask about what is being covered by the policy and what duties you have under the policy. This way, you can see what other risks you may need to mitigate with your internal policies and procedures or an outside vendor.

There is no one-size-fits-all solution

This article's advice is meant to be a primer to help organizations understand the risks associated with data loss. It is ultimately up to each organization to decide what is best for its operations. Talk with your leadership, compliance, and IT teams to develop a solution that is the right fit for your organization.

Takeaways

- Security practices must be shared, embraced, and followed by all.
- If it is in practice at your organization, stop to consider if Bring Your Own Device is still the right option.
- Aim for continuous improvement in your information technology department.
- Be prepared with logging, backups, and insurance.
- Choose the solutions that are right for your organization.

---

[1] Laura LaBerge, Clayton O'Toole, Jeremy Schneider, and Kate Smaje, *How COVID-19 has pushed companies over the technology tipping point—and transformed business forever*, McKinsey & Company, October 5, 2020, https://mck.co/3eCj17K.

[2] Sean Gallagher, "WannaCry? Hundreds of US schools still haven't patched servers [Updated]," Ars Technica, May 21, 2019, https://bit.ly/3p462QM.