COSMOS
Navigate the Compliance Universe

# 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.