CYBERSECURITY and Compliance in the Face of COVID-19

By Scott Kaylor

The COVID-19 pandemic and the subsequent urgency to move employees en masse to a work-from-home environment pushed technological boundaries never before tested properly. The transition has gone smoother for some than for others, but there are some critical items all organizations need to keep at the forefront of their minds.

CYBERCRIMINALS CAPITALIZING ON THE PANDEMIC

In the midst of a global pandemic, there is a prime opportunity for hackers to attempt to exploit the situation. As our focus is on the effects of the virus on our organizations, our communities, and our families, our overall cyber guard could be down simply due to distraction and a little ingenuity on the criminals' behalf. Much like the recommendation to take a little longer washing your hands, it is imperative that everyone take a little longer when checking email or browsing online.

There have already been a number of instances of successful malware deployments while disguising themselves as information about the pandemic. For example, coronavirusmap.com.exe is a real-time map that pulls information from the CDC about coronavirus cases and visually illustrates the impact. However, this map also steals information from the user's browser. It is imperative to ensure sources are legitimate and secure.

Ensuring legitimacy also applies to emails. Now more than ever, cybercriminals are phishing for victims. We are living in a time of distraction, and when our focus is more so on the operation of our organization and the health of our loved ones, it is quite easy to open an unexpected email and click on the included link or open an attached file.

Our guards cannot be down. It is critical we survey each email with a discerning eye. If the email wasn't expected, don't open it. If it is from a known contact, be sure to hover over the link to double-check it is directing you to a safe site. And practice caution when opening any attachments, perhaps verifying directly with the contact that the attachment is safe.

The threats are evolving as criminals are also preying on the charitable spirit. People are raising funds to help those affected by COVID-19. As with the widespread fires in Australia, both legitimate and illegitimate campaigns have emerged. Criminals have started up GoFundMe pages promising to donate 100% of the contributions to aid the relief efforts—only for the money to just disappear. While raising funds for those impacted is always welcome, a little bit of research into the credibility of the campaign is key to ensuring the funds are truly getting to those in need.

However, there are a plethora of legitimate cyber resources that can provide real-time threat information that everyone can use to defend their organizations—and even their families while online. Education is key. Knowledge of the threats and awareness of using best practices online will help navigate the cybercriminal minefield.

STAYING COMPLIANT WHILE REMOTE

Many organizations have adopted employee home offices for the foreseeable future. This is an incredibly logical solution to the pandemic, but it does open the door to some security and compliance concerns. While working inside the walls of your organization, security protections have been put in place to provide a hedge between trusted and untrusted. When employees are moved to an untrusted place, such as a home office, it is imperative to either fortify the new location or leave what would otherwise be vulnerable services within the trusted environment. With PCI compliance, that is every bit the case.

PCI-DSS is the shorthand for Payment Card Industry Data Security Standard, which is a set of standard security practices put in place to ensure that the acceptance of credit card payments, along with the processing, storage, and transmission of credit card data, is done in a secure manner. If there's one thing you need to know about PCI compliance, it's that as the merchant of record-taking card payments you need to be PCI compliant. Ensuring that you are using PCI-compliant solutions to process payments is important, but ultimately the onus is on the merchant to secure any in-scope components and environment changes.

Anyone involved in payment card processing needs to ensure that the PCI Data Security Standards are being met. PCI compliance involves people, processes, and systems. The manner in which the card numbers are captured will make a difference in how much effort is required on your part to protect the card data. Be aware that there very well could be penalties from each card brand for non-compliance, upwards of $80,000 per month, depending on your merchant level.

Much like keeping track of your tax information, PCI compliance is not a one-and-done transaction. There are many aspects of this culture of security that require you to keep on top of the entire environment, including the information itself, your network, and even your personnel. You must ensure that each component of your entire business environment is kept secure and is not the weak link to a credit card data breach. PCI must be part of your business-as-usual processes, and awareness as security must be woven into the very fabric of your culture.

With your organization now being in the employee's home, it is critical to be aware of the implications in regard to PCI compliance. For instance, if your organization set up Verifone to connect to the office network to take payments, which keeps the computer network out of PCI scope, accepting a call over the phone likely means that phone system is in PCI scope, as is already often the case.

The cardholder data (CHD) is still transmitted over the phone which is then brought into PCI scope. If you decide to use an online bill payment tool or virtual terminal in a browser, the computer would be in PCI scope just as it would if you were in the office. Using remote desktop protocol or a thin client like a Citrix workstation would help minimize exposure—but remember that the potential for keyboard logging and even memory scraping would be a concern. Applicable PCI requirements are still in full effect.

A TRUE TECHNOLOGY PARTNER

Sound cybersecurity practices are not critical only during a pandemic but also in times of normalcy. Ensure your software vendor has sound security policies to protect your organization's vital information. Furthermore, an ideal technology partner can also offer essential security services and valuable staff cyber education tools for your organization.

Additionally, the ability to direct your customers to PCI-compliant e-commerce solutions is unquestionably the most secure and least disruptive way for your customers to make a payment. E-commerce solutions allow customers to make payments to those avenues without compromising your PCI compliance or their CHD. Directing customers to these solutions maintains continuity with already-in-place solutions and does not require you to compromise your PCI compliance or put extra strain on employees or your network. NWPPA

Scott Kaylor is the cybersecurity and networking services manager at National Information Solutions Cooperative (NISC), a true technology partner offering robust, fully integrated solutions from cybersecurity to e-commerce, and all elements in between. Kaylor can be contacted at Scott.Kaylor@nisc.coop.