Cybersecurity and data privacy trends to expect in 2020

Dominic A. Paluzzi, Christine N. Czuprynski, Emily A. Johnson | Tuesday, January 28, 2020

In recognition of International Data Privacy Day, McDonald Hopkins has identified the top data privacy and cybersecurity trends for the coming year. In October, we looked at the 2019 trends and made some predictions about what could be in store for 2020. In the fast-paced, ever-evolving world of data privacy and cybersecurity, it is not hard to believe that a lot has happened since then. Read on for our insights on the current risks facing all organizations.

1. **Exploitation of remote access vulnerabilities**
   Companies hoping to attract the best and brightest employees are assessing non-monetary perks that can help retain talent. One of those perks is allowing employees more flexibility, including working remotely. Allowing employees to work remotely requires a business to implement a process to access the network, email and files. One way that criminals access systems and deploy malware or compromise email accounts is through these remote tools. As businesses move in the direction of allowing more of their workforce to access the network remotely, care should be taken to ensure the remote access tool is secure and any exploitable vulnerabilities are minimized.

2. **Election security**
   In this presidential election year, the security of the nation's election systems is critical. State and local election officials have been in high gear since the 2016 presidential election to update election systems and take steps to ensure that those systems are not vulnerable to fraud or interference. Some updates to election systems have been imposed by court order, while others have been undertaken voluntarily. Election security is also a top priority for the U.S. government. We expect that as primary voting gets underway, and as we move closer to the general election in November, the

focus and scrutiny on these systems will continue to increase.

3. **State-sponsored cyber attacks**
   In the wake of the killing of Iranian military commander Qasem Soleimani and rising tensions with Iran, the U.S. Department of Homeland Security warned companies to prepare for possible cyberattacks perpetrated by Iran. State-sponsored cyber attacks have also come from Russia, China, and North Korea, and have impacted a variety of types of businesses from financial institutions to utility companies. As part of an overarching cybersecurity and data privacy program, entities should be conducting data inventory and risk assessment of the specific, unique threats they face.

4. **Regulatory scrutiny and state data privacy/security legislation**
   The California Consumer Privacy Act (CCPA), a comprehensive data privacy law that is aimed at providing California residents more control over their personal information and how it is collected, used, shared, and sold, became effective Jan. 1, 2020. Most businesses worked throughout 2019 to update internal policies and procedures relating to notice of their privacy practices, and established mechanisms and processes for allowing individuals to request access to and deletion of their personal information. Many other states (including Nebraska, New Hampshire, Washington, Florida and Virginia) are considering CCPA-like legislation to provide their residents with that same level of transparency and control. We are keeping a close eye on the status of those bills.

Federal and state regulators are also increasing scrutiny of data breaches and other security incidents. Regulators expect businesses to implement policies and procedures to detect potential breaches and to respond quickly. The response includes engaging legal and forensic experts to analyze the incident, and, most importantly, to get notification of the incident out to impacted individuals, where required, as timely as possible.

5. **Ransomware**
   Ransomware continues to impact many organizations, from private businesses to public universities, from municipalities to hospitals. Organizations of all sizes have been impacted by ransomware, and no industry is immune. An alarming trend that began in late 2019 is the introduction of ransomware variants that are designed to capture and release data in the event that the ransom is not paid. Until recently, the criminals perpetrating these attacks typically did not access or acquire any data. Their motivation was purely monetary – getting paid to provide the key to decrypt the information. As businesses have taken steps to solidify back-ups so that payment of the ransom is not necessary, some criminals have shifted tactics in an attempt to get paid no matter what. Legal and forensic experts are critical in these incidents to help impacted organizations understand the nature and scope of any attack, and the potential consequences of ignoring the threat actors.

6. **Business email compromise**
   Business email compromise – an oldie, but a goodie. Criminals continue to compromise email accounts and insert themselves into legitimate conversations to redirect wire transfers, invoice payments, or W-2s. This type of compromise hasn't gone away because it works – criminals successfully pose as legitimate business customers or vendors and trick individuals into sending payments to their "new" bank account. Businesses should encourage their employees and staff to take some offline steps to confirm changes to wire instructions, bank accounts for vendors, or strange or urgent requests being made internally. These offline steps include calling appropriate contacts, or, if the sender of the suspicious email is in the same physical location, walking down the hall to discuss any concerns.

   Remember that criminals get into email accounts by exploiting remote access vulnerabilities (see above), through successful phishing campaigns, and by brute force attacking other areas of a company's network. In addition to taking steps to mitigate the harm once a criminal is in, businesses should take steps to shore up their security to prevent unauthorized access in the first place. These attacks can be particularly detrimental to healthcare entities, who are subject to both HIPAA and state privacy laws, and can result in government investigations if the e-mail boxes contain significant personal information. Businesses in the healthcare sector should evaluate their internal transmission of patient information to reduce the impact of a business email compromise.

Count on the McDonald Hopkins Data Privacy and Cybersecurity team to stay on top of the 2020 cyber trends and we will provide the very latest as it unfolds.

Dominic A. Paluzzi

Christine N. Czuprynski

Emily A. Johnson