HR Heads to the Front Line as Cybercrime Combatant

Unfortunately, many HR pros still view themselves in a traditional role, leaving cyber risk management to other departments.

In the war against cybercrime, human resource professionals are being asked to join their companies' cyberdefense as "boots on the ground," at the front lines. The reason: HR is home to valuable personal and corporate data, systems and processes that cybercriminals target day in, day out.

Whereas IT and other technology specialists work daily with the thought of protecting corporate networks, in today's cyber risk-laden world, HR professionals, despite their limited technical expertise, must work to protect sensitive data and operate in ways that mitigate the potential for attacks by technologically proficient cybercriminals.

Take cloud-based HR systems. Because of minimal hardware costs, affordable subscription rates and scalability, these systems are utilized widely by small to middle market enterprises as well as by large corporations. Many of the core back-office HR functions, such as benefits management, time and attendance, have migrated quickly to the cloud after leaping from antiquated, paper-based spreadsheets to on-premises software.

In a recent worldwide survey of 1,100 senior IT security executives by Vormetric, 85 percent revealed they keep sensitive data in the cloud and 70 percent admitted they are very concerned about the security of the data in this environment.

This survey also found that 70 percent of respondents are concerned about security breaches and attacks at the cloud service provider, while 66 percent worry more about vulnerabilities from shared cloud infrastructure.

These fears are not unfounded. Left unchecked, cloud systems have become a potential gateway for cybercriminals to access such personally identifiable information as employee information, social security numbers, credit card numbers, bank account details, medical records, salaries and other financial data.

Social engineering schemes, with scammers posing as company executives via email (also known as "spoofing"), are moving from their original ploys of inducing a bank transfer under false pretenses to seeking to induce HR personnel to click on a deceptive link (opening ransomware) or to send sensitive payroll data, including W-2s. The seriousness of this was driven home earlier this year when IRS Commissioner John Koskinen warned company executives and HR professionals that criminals are focusing their schemes on company payroll and HR departments.

"If your CEO appears to be emailing you for a list of company employees, check it out before you respond. Everyone has a responsibility to remain diligent about confirming the identity of people requesting personal information about employees," Koskinen said.

The Toll of Cyberattacks

So far this year, a record amount of personal information was stolen from W-2s and used to file fraudulent tax returns.

In May, ADP, the giant payroll processing company that services more than 640,000 clients, divulged a breach that exposed tax information of employees of some of its clients. The cyberthieves reportedly gained access to the tax data through an external W-2 online portal maintained by ADP.

The total W-2 social engineering and fraud impact to date, for the most recent year available (2014), is mind-boggling. According to the IRS, $3.1 billion was paid out under fraudulently filed W-2's. The 2015 tax year is expected to see this number increase dramatically.

In other recent cases, cybercriminals are looking to target HR data or HR network access for ransom. Various types of ransomware — software used to encrypt files and lock computer screens — have been used to attack HR systems, with levels of success. Symantec reported that in early 2016, ransomware found new targets and moved beyond its focus on PCs to smartphones, Mac and Linux systems.

The Industry's Response to Date

Despite the increased vulnerability of HR systems, many HR professionals still view themselves in the traditional role of workforce management, choosing to leave cyber risk management to other departments, notably IT.

According to a recent IBM security study released this year, 57 percent of chief human resources officers globally have rolled out employee training that addresses cybersecurity. However, the respondents' positive percentages dropped noticeably when asked if they provided cybersecurity training that included measurable, results-based outputs, or if there was reinforcement throughout the year that provided more than a once a year cybersecurity training.

Some HR departments operate under the incorrect assumption that an HR back office cloud service provider is automatically responsible for employee data breached or exposed. In fact, should lax security measures or a breakdown in security protocols of an HR cloud or an IT service provider allow cybercriminals to steal employee data or breach personal information, the company that owns the data — and by extension the HR personnel responsible for the data — will incur the obligations (and expense) for notifications, credit monitoring and other issues.

In other words, just because a company hands over data to a cloud service provider doesn't reduce or eliminate its liability. This is an emerging contractual issue that HR, legal and the C-suite need to work together to address in all HR IT service contracts.

The costs to notify, provide credit monitoring and hire third-party forensics experts can be staggering, potentially costing millions of dollars in the event of a successful cyberattack. Additionally the resulting business interruption expense could force small to medium-sized businesses to close.

Given the growing financial exposure and traditional duties in human resources (e.g., screening new employees, onboarding, training and the administration of sensitive HR data), HR must incorporate comprehensive cyber risk management practices across the enterprise. This is crucial; the study by IBM shows more than 20 percent of data breaches at work can be attributed to careless employee mistakes.

HR Roles Need to Evolve

The IBM report urged key executives in human resources, finance and marketing departments to be more proactive in security decisions, coordinate plans internally and to be more engaged in cybersecurity strategy and execution with the C-suite and IT.

This means HR personnel should not only stay abreast of proper security processes when it comes to accessing sensitive employee data, but they should be able to communicate updates about cyber threats effectively to the enterprise, to current and new employees, and contractors.

For example, during the onboarding process of a new employee, HR personnel can begin cyber risk education by delineating corporate policies on email sharing, network access, social media policies, what to do if there is even a doubt about the veracity of an emailed instruction, and company best practices on the use of cybersecurity tools. On a continuing basis, HR departments can facilitate cyber risk-focused internal communications to employees, particularly when the information relates to cyberattack prevention and training against emerging threats.

Another crucial emerging HR responsibility is ensuring that proper steps are taken to prevent former employees and contractors from continuing to have access to corporate networks. While this requires HR and IT to be aligned in real-time to minimize lag

that could allow for a security exploit, the threat is real — a survey by Heimdal Security found that nearly 60 percent of fired employees steal important corporate data, including HR data, after departing their position.

Given their growing importance on the front lines in the war on cybercrime, it is imperative for HR professionals to evolve in their roles and become valued security partners within their organizations.

As HR systems incorporate new technologies, HR and IT, along with senior enterprise management, must partner together strategically to combat cyber threats. We're all in this together now.