As seen in the January 13, 2017 issue of

BUFFALO
BUSINESS FIRST

COMPANY POLICIES

Employees play key role in cyber safety

BY MICHAEL PETRO
mpetro@bizjournals.com
716-541-1654, @BLJ_Mpetro

MICHAEL PETRO

Attorney Kevin Burke says he's fascinated by how often cyber breaches occur and the variety of entities and individuals targeted.

The email controversy that followed Hillary Clinton for much of the presidential campaign provided some valuable lessons for companies facing the constant threat of cyber and data breaches.

Employers need clear, written policies on cyber security relating to the use of company email, servers and confidential business.

And the policies must be followed to optimize these safety measures, said Kevin Burke, a partner and litigator at Lippes Mathias Wexler Friedman.

He said he is fascinated by everything going on in this realm, including the results of Clinton's use of a personal server when she was U.S. secretary of state.

"These breaches keep happening," said Burke, a labor and employment attorney. "When it happens to mom-and-pop stores, I'm sure that they weren't up to code, so to speak. But when it happens to Visa and Facebook and Target, which is becoming almost old news by now, it's just amazing.

"It's happening to government; it's happening to everyone," he said.

Clinton reportedly used her own server to conduct daily business and official communication instead of using official State Department email accounts maintained on federal servers. There was a plan in place but the practice superseded it, according to Burke.

If the plan is not followed, employee handbooks and agreements are meaningless, he said.

The tone needs to be set from the top down.

"Sure, they may all know that they're not allowed to use company email or a company-issued iPhone or mobile devices for personal use, but everybody does. And the worst is when they see the people in the corner offices doing it," he said. "You can't have different rules for the bosses than you do for the rank and file."

John Horn, managing partner of the Buffalo office of Harter Secrest & Emery, said a key takeaway from the Clinton email breach – for which U.S. intelligence agencies say Russia is responsible – is that failing to protect private information can be costly.

He said law firms, accounting firms, municipalities and government sometimes don't have a handle on their data inventory, what they're collecting, why they're collecting it and how to properly protect and then destroy it.

Horn said it's imperative to have everyone at a business who touches data in on the conversation at an early stage so they understand how it is linked to the company's continued success.

"They are organization changing, they are deal busting, they are growth stopping, so the stakes are huge," Horn said. 'The unwillingness or inability to think carefully and strategically about protecting private information has huge costs associated with it."

Michael McCartney, president of Digits, a division of Avalon Document Services, said this issue is a matter of national security.

Too many industries don't take information security seriously enough, he said. Many simply assume they are not a target and question what a hacker would want with their company information.

But hackers "want everything," McCartney said, including personal and health care information, as well as the company process, procedures, methodology and, for government-sponsored international hackers, a sense of the way things are done in the United States.

"We are being attacked," he said. "Essentially, people think that when we pulled our troops out of Iraq and Afghanistan, the wars were over, when they really just shifted theaters. They moved from a ground war to an electronic war."

According to McCartney, 60 percent of small to midsize companies that experience a breach will be out of business in six months or less. And 98 percent of the U.S. economy sits on the backs of those companies.

In the last year, cyber criminals that attack businesses with one to 250 employees rose from 18 percent to 43 percent. The average cost to businesses to recover from a breach has risen to $3.9 million and the average time to identify a breach is 191 days.

"A bad guy can steal a whole bunch of stuff in six and a half months," McCartney said.

Many clients express concern about their employees' use of personal devices, Burke said. And while some reimburse employees for the work they conduct with their personal devices, that can lead to a host of problems. The person uses one device that's on multiple servers, including the work server. The other servers may not have a firewall.

"There is a tension between convenience and efficiency and security. And we're not at that place yet, unfortunately, where the two are the same," he said. "We're getting there, but it feels like the bad guys are one step ahead of the good guys because there is more money in it for the bad guys."

He advises companies to develop a plan and stick to it. Incident-response plans should be crafted and reviewed by the HR and legal departments and then signed by all employees.

"Companies can't afford to spend $2 million to $3 million on beefing up their firewalls, but what they can do is beef up their security policy and have a meeting in the first quarter to remind people of the basics," Burke said.

Written policies will spring from gaining a better understanding of data inventory and the compliance requirements that come with it, according to Horn.

Businesses also should understand that clients regard this as an important consideration for prosperity.

While there are hardware and software innovations and enhancements that can safeguard against data breaches, a major vulnerability for a company remains the workforce, Horn said.

Ransomware, for example, can lead to the lockdown of a company's computer system. Hackers often access the system using phishing scams.

"We think the next gain companywide and industrywide is going to be in the communication of the policies – conveying the why behind the policies and then drilling the policies," Horn said.

According to McCartney, since there is virtually no way to prevent a breach, even for major companies that spend millions to protect their information, the focus has to move to detection and having a comprehensive and immediate response plan.

A risk assessment can identify vulnerabilities and help manage and mitigate exposure, he said.

Computer systems should be monitored for suspicious behavior, he added. Most are only monitored for viruses.

A typical IT department is not in the business of security; it's about availability to the network, according to McCartney. A third party could provide those services by putting sensors in the computer system to minimize the damage.

"The only way we're going to win this thing is through detection and response," he said. "We have to do a better job of detecting this stuff quicker and responding more comprehensively. It makes all the difference in the world."