# LI companies focus on weak link in cybersecurity: Employees

**KEN SCHACHTER** SEPTEMBER 22, 2017

Secure Decisions' Trevor Bidhadar shows the Comic-BEE project

Cybersecurity experts and companies on Long Island are looking for ways to shore up the weakest link on company computer networks: the employee.

Local cybersecurity professionals are creating interactive comic books, testing employees with simulated phishing emails — tailored messages that seek to obtain key information, such as passwords — and seeking to convince top executives that the threat of business disruption from hacking requires their attention.

"The biggest problem is not the technology; it's the people," said Laurin Buchanan, principal investigator at Secure Decisions, a division of Northport software developer Applied Visions Inc.

Sixty percent of cyber-assaults on businesses can be traced to insiders' actions, either inadvertent or malicious, according to a 2016 study by IBM Security.

The average cost of a data breach for U.S. companies is $7.4 million, or $225 per lost or stolen record, a June 2017 study by IBM and the Ponemon Institute, a Traverse City, Michigan, researcher, found.

Costs related to data breaches can include the investigation, legal costs to defend against and settle class-action lawsuits, credit monitoring for affected customers, and coverage of fraud losses. Harder to gauge is the cost to a company's reputation.

One of the largest hacks ever was disclosed this month, when credit reporting company Equifax Inc. revealed that sensitive data from 143 million consumers, including Social Security numbers and birth dates, was exposed. A stock analyst from Stifel Financial Corp. estimated that the attack will cost Equifax about $300 million in direct expenses. Investors seem to think the incident will have a much greater impact on the company: Equifax stock has lost almost $5 billion in value since the breach was disclosed Sept. 7.

And the Securities and Exchange Commission said on Wednesday that hackers who broke into its disclosure filing system may have used the information gained there to make illegal trades.

Cybersecurity is on the agenda of Long Island companies, large and small.

"If a [type of] cyberattack exists, it has happened on Long Island," said Nicole Della Ragione, a member of Uniondale-based Ruskin Moscou Faltischek, PC's cybersecurity and data-privacy group.

At a seminar in Garden City this month, Henry Prince, chief security officer at Shellproof Security in Greenvale, explained how in a

ransomware attack — one of many types — cybercriminals can buy specialized tools such as those used to send phishing emails. The easy availability of that software means that hackers require "no programming experience," Prince said.

Phishing emails can be blocked by company email filters, firewalls and anti-virus software. But if one gets through and an employee clicks on the link in the phishing email, the business' network is compromised. Hackers can then encrypt files, preventing access to them by the company and crippling the business, Prince said at the seminar.

Hackers then can demand payment, typically in an untraceable cryptocurrency like Bitcoin — a digital asset that uses encryption — before agreeing to decrypt the files.

"Ransomware is a business to these people," Prince said. "Ninety-nine percent of the time, ransomware requires user interaction to infect."

Della Ragione echoed that sentiment: "The greatest risk at a company is the employees. Training employees is one of the best steps in shoring up your defenses."

In response, many local experts and companies focus on teaching employees how to resist hackers' tricks.

Secure Decisions has developed interactive comics to teach employees ways of detecting "phishing" emails and other hacking attempts. The company has gotten more than $1 million for research related to the interactive comic project, known as Comic-BEE, from the Department of Homeland Security, as well as a grant for $162,262 from the National Science Foundation.

The comics, inspired by children's "Choose Your Own Adventure" books, feature different plots depending on the reader's choices.

“If you can give people the opportunity to role-play, some of the exhortations by the experts will make more sense,” Buchanan said.

The comics are being field-tested at several companies and Stony Brook University. They were featured in July at a DHS cybersecurity workshop in Washington, D.C.

Radu Sion, a computer science professor at Stony Brook and director of its National Security Institute, which studies how to secure digital communications, acknowledged that security is far from a priority for most users.

“Ultimately, the average Joe doesn’t care,” he said. “You [should] treat the vast majority of your users as easily hackable.”

Northwell Health, the New Hyde Park-based health care system that is the largest private employer in New York State, is trying to find and get the attention of those inattentive employees.

Kathy Hughes, Northwell vice president and chief information security officer, sends out “phishing simulations” to the workforce. The emails are designed to mimic a real phishing campaign that seeks passwords and personal information. In April, for instance, Northwell sent out phishing emails with a tax theme.

Hughes collects reports on which employees take the bait by user, department and job function.

“We present them with a teachable moment,” she said. “We point out things in the email that they should have looked at more carefully.”

The emails are supplemented with newsletters, screen savers and digital signage reminding users that hackers are lurking. Another tool: Non-Northwell emails have an “external” notation in the subject line, making it harder for outsiders to pretend to be a colleague.

“We let [the employees] know that they are part of the security team,” she said. “Everybody has a responsibility for security.”

One of the most important constituencies for security is top executives.

Drew Walker, a cybersecurity expert at Vector Solutions in Tampa, Florida, said many executives would rather not know about vulnerabilities to their computer systems, because knowledge of a hole makes them legally vulnerable and casts them in a bad light.

“Nine times out of 10, they don’t want to hear it,” he said. “It makes them look bad.”

Richard Frankel, a former FBI special agent who is of counsel at Ruskin Moscou, said that company tests of cybersecurity readiness often snare CEOs who weren’t paying attention to training.

But attorney Della Ragione said high-profile attacks are getting notice from executives.

“Everyone’s consciousness is being raised,” she said.

Data leaks at Long Island companies have caused executives to heighten security.

In 2014, Farmingdale-based supermarket chain Uncle Giuseppe’s Marketplace said that foreign hackers had breached the credit card database of three stores. Joseph Neglia, director of information technology at Uncle Giuseppe’s, said that after the data breach, which affected about 100 customers, the company began scheduling “monthly vulnerability scans” and upgraded its monitoring and security systems.

In June 2012, Bethpage Federal Credit Union acknowledged that an employee’s computer error allowed the personal information of nearly 86,000 members to be visible on the internet for a month. Bethpage president and chief executive Wayne Grosse said in a statement that the

credit union took “immediate action” when it learned of the data breach to ensure customers’ information was not at risk, and “implemented even more rigorous internal security” to safeguard information.

Earl Crane, former director for federal cybersecurity policy on the White House National Security Council during the Obama administration and founder of Emergent Network Defense, based in Austin, Texas, argues that artificial intelligence can help thwart cyberattacks.

Crane said that AI systems that flag unusual patterns on computer networks have become mature enough to have a place — along with firewalls, intrusion detection systems and anti-virus software — in enterprise cybersecurity.

If the National Security Agency had an artificial intelligence system in place, “it would have caught” Edward Snowden, a former contractor who used specialized software to gather classified files from the spy agency and release it to the public.

Crane said that insiders with a malicious intent pose a grave danger.

In January, Michael Meneses, a former software programmer at Hauppauge-based Spellman High Voltage Electronics Corp., was sentenced in U.S. District Court in Central Islip to 12 months and one day and ordered to pay more than $19,000 in restitution for hacking the company after he quit in 2012.

For businesses, Stony Brook’s Sion said, the cybersecurity threat is real and immediate.

“I need one second with your machine to compromise it forever and ever,” he said. “It’s an uphill battle.”

You are the weakest link

60%: Proportion of cyber assaults traced to insider mistakes or malicious actions

$7.4 million: Average cost of a data breach for U.S. companies

Sources: IBM; Ponemon Institute