View this email in a web browser

WSJ PRO CYBERSECURITY

IN THIS EMAIL→ Commentary & Analysis More from Dow Jones Editor's News Picks

HIGHLIGHTS

COMMENTARY & ANALYSIS

Health Care Risk Underlined By Insider Threat Finding

By Jeff Stone

In 2016, internal employees and trusted business associates caused more data breaches in the health care industry than outside attacks, according to a new study viewed by WSJ Pro.

Forty-three percent of the health care breaches that occurred last year started with someone inside or with ties to the breached organization, according to a new study from security software vendor Protenus. The firm examined data from 450 breaches at hospitals, at health insurers, and other services that aim to protect sensitive patient information. Insiders were blamed for 192 of those 450 incidents, including 99 accidents and 91 cases of "insider wrongdoing."

Compare that to the 27% of breaches pinned on malicious hackers, and the 19% blamed on loss and theft. The cause of the remaining 11% of breaches could not be determined.

"We talk so much about hacking, but it's actually insider threats that are dominating the picture," said Robert Lord, Protenus chief executive. "And if you

look at the insider threat in health care, there's an average of 607 days between the breach and detection."

Digital insecurity is a problem in every industry, but health care faces unique challenges in protecting patient health information, intellectual property, and other sensitive data. Bob Chaput, founder of Clearwater Compliance, which aims to help secure hospital technology, said the industry has prioritized compliance, but undervalues security. The 1996 Health Insurance Portability and Accountability Act, for instance, set a baseline standard for protecting patient privacy, and the 2009 Health Information Technology for Economic and Clinical Health Act set new standards for record digitization.

Many executives, hospital administrators, and insurers see HIPAA and HITECH as end goals, Mr. Chaput said, rather than a baseline that can be improved upon.

"I'd put forth that health care is a decade behind when it comes to adopting information technology, and I'd say they're multi-decades behind when it comes to security," he said."For instance, chief information officers are still not given enough funding."

Cultural and funding problems becomes even more serious upon considering the type of threats against the medical industry. Health records can be monetized by cybercriminals, hackers can exploit connected medical devices, and nation states almost certainly have an interest in collecting American's health records--a new investigation determined a foreign government was behind the hack on Anthem health insurance. Often, health care professionals are working in stressful environments where they simply don't have the time or resources ability to undergo cybersecurity training.

"The nature of being open, connected, and working with many different parties really just opens you up to more adversaries and potential for problems," said Chris Carlson, vice president of the cloud security company Qualys. He added security problems exist "everywhere" in health care, because of outdated technology and the number of motivated adversaries.

No sweeping solution for the industry is on the horizon. But Mr. Carlson explained that awareness is growing thanks to headlines about the cyberattacks that have hit Anthem, Hollywood Presbyterian Medical Center, BlueCross Blueshield, and others. "When everything goes right, nobody knows you're doing

it right. But when it all goes wrong, we know something is wrong."

Other experts recommend a mindset shift that regards security as an issue that, if not administered correctly, could lead to lawsuits, job loss, or worse.

"It's a huge risk if a hacker changes my blood type the night before I'm scheduled to have a transfusion,"said Mr. Chaput. "We need to move forward from thinking about this in terms of compliance to patient safety. Minimally, security needs to become a team sport not just involving the IT team but the executive suite, risk management, the compliance team and the legal team."

(Jeff Stone writes exclusively for WSJ Pro Cybersecurity. He previously covered privacy, international hacking groups, bug bounties, and a range of related topics at media outlets including the Christian Science Monitor and the International Business Times. Write to Jeff at jeff.stone@wsj.com)

MORE FROM DOW JONES

Rubin's Take: Cybersecurity Professionals Wanted

By Gabriel T. Rubin

An employee in a server room at a company in Bangkok, Thailand. More than half of the global firms polled in a recent study said they had 'at least one security event in the past year' and attributed it to a 'lack of security staff or training.' ATHIT PERAWONGMETHA/REUTERS

A series of high-profile cyberattacks on major corporations and financial institutions—including J.P. Morgan Chase & Co. and Yahoo Inc., among many others—have convinced executives that cybersecurity is a fundamental part of their risk management responsibilities. But what's less clear is whether there are enough trained cybersecurity professionals to build and maintain resilient cyber-infrastructure at those firms.

More than half of the 437 global firms—54%—polled in a recent study said they suffered "at least one security event in the past year" and attributed it to a "lack of security staff or training." According to the report from the Information Systems Security Association and analysis firm Enterprise Strategy Group, 56% of respondents said their firms didn't provide their cybersecurity teams with the right level of training to keep up with the developing threat landscape. The study showed that corporate cybersecurity teams are overworked and undertrained, putting consumer financial information and other data at risk.

Much of dealing with the cybersecurity issue has involved developing industry-wide but voluntary sets of best practices, rather than the imposing regulatory requirements and building an enforcement regime. While those voluntary

standards are crucial for establishing uniform priorities and rapid-response procedures, they will not upgrade cyber-infrastructure on their own.

Troy Leach, chief technology officer at the PCI Security Standards Council, which sets standards for the credit-card industry, said the larger problem for firms was that they continue to treat cybersecurity as a discrete problem rather than as a "baked in" part of their other duties.

"We're really going to have a security problem because there are just not enough professionals to design these [products and web platforms] correctly, especially systems that can accept payments," he said in an interview. Cybersecurity needs to be a part of platform and product design from the beginning, he said. Too often, firms instead try to enhance the security of existing infrastructure, which can be more costly and difficult than designing systems with security in mind from the outset.

Given the interconnectedness of the financial system, the financial industry faces a particular challenge in making sure its cyberdefenses can adequately respond to threats that could put the entire system, not just individual firms, at risk.

These firms would be well-served if they stopped taking a cookie-cutter approach to cybersecurity, said Joel Rasmus, managing director of the Center for Education and Research in Information Assurance and Security at Purdue University.

"The industry has put way too much emphasis on certification rather than knowledge," he said. When hiring information-technology employees, certifications in cybersecurity are highly valued—and grossly overestimated, Mr. Rasmus said. Firms would be better served if they hired professionals who demonstrated cybersecurity capabilities that would actually help them on the job, and firms should institute their own training programs for all IT employees to make sure that the firm's cybersecurity needs are a priority at every stage of their product development and systems management.

Until then, Mr. Rasmus said, firms should expect big, debilitating cyberattacks to continue.

Write to *Gabriel T. Rubin at gabriel.rubin@wsj.com*

FBI's Comey Says Republican Data Also Hacked by Russians

By Devlin Barrett

FBI Director James Comey testifying before the Senate Intelligence Committee in Washington, D.C., on Tuesday. JIM LO SCALZO/EUROPEAN PRESSPHOTO AGENCY

FBI Director James Comey said Tuesday that Russian hackers successfully hacked some Republican groups and campaigns, though officials said the Russians revealed much less of that material compared with the volume of disclosures made about Democrats' emails.

Mr. Comey, in his first public appearance since the election, appeared with other intelligence chiefs before the Senate Intelligence Committee to discuss the alleged Russian hacking of the Democratic National Committee and senior party operatives with the goal of tarnishing Hillary Clinton's presidential bid.

Committee Chairman Richard Burr (R., N.C.) asked Mr. Comey whether Republicans were also targeted by Russian intelligence.

"There were successful penetrations of some groups and campaigns, particularly

at the state level on the Republican side of the aisle, and some limited penetration of old [Republican National Committee] domains," Mr. Comey said.

Those domains, he added, "were no longer in use" at the time of the hack. "Information was harvested from there, but it was old stuff," Mr. Comey said. "We did not develop any evidence that the Trump campaign or the current RNC was successfully hacked."

The Wall Street Journal previously reported that an email account linked to a long-departed RNC staffer was targeted. Officials familiar with the probe have also said the Russian hacking effort was generally much less extensive against the Republicans than the Democrats.

The panel's top Democrat, Sen. Mark Warner of Virginia, said he didn't want to "re-litigate" the presidential election, but some lawmakers raised Mr. Comey's much-debated decision to announce, less than two weeks before Election Day, that the Federal Bureau of Investigation was investigating newly discovered emails that could be connected to a dormant probe into Mrs. Clinton's use of a private server when she was secretary of state.

Mr. Comey, pressed on whether the FBI had investigated possible links between the Russian government and people connected to Mr. Trump, told senators, "Especially in a public forum, we never confirm or deny any investigation."

That prompted Sen. Angus King of Maine, an independent who caucuses with the Democrats, to respond, "The irony of you making that statement here, I cannot avoid," alluding to Mr. Comey's public statements to Congress about the Clinton probe.

Mr. Comey later joked about the political heat he had taken about his handling of the Clinton matter, saying, "I hope I've demonstrated by now that I'm tone deaf when it comes to politics."

Sen. Kamala Harris (D., Calif.) charged Mr. Comey created a "new standard" for discussing probes when it came to the Clinton case, and said she wanted to see a similar sense of urgency about Russian involvement with U.S. elections.

"I'm not sure I can think of an issue of more serious public interest than this one," she said.

The bulk of the hearing focused on the implications of Russia hacking and propaganda targeting U.S. democracy. Sen. Marco Rubio (R., Fla.), who lost the Republican primary to Mr. Trump, said he thought the Russians had been "pretty effective" in their hacking.

"It sounds like they achieved what they wanted—to get us to fight with each other over whether our elections were legitimate," he said.

Mr. Comey, like the other intelligence chiefs, said he had never seen this level of Russian interference in U.S. elections. Mr. Comey testified alongside James Clapper, director of national intelligence, and the heads of the National Security Agency and the Central Intelligence Agency.

Mr. Clapper said Russian President Vladimir Putin and Russian officials didn't expect Mr. Trump to win, particularly when the hacking began. "They thought he was a fringe candidate," Mr. Clapper said.

The head of the CIA, John Brennan, said he spoke to his Russian counterpart in August, warning him that the U.S. knew Russia was behind the leaking of Democratic emails, and warning they should stop. The Russian official denied involvement, but said he would relay the message to Mr. Putin. After that discussion, the leaks continued.

Mr. Comey also testified that as the FBI probed the alleged Russian hacking, DNC officials didn't allow agents to access the committee's servers. Party officials instead hired a cybersecurity firm with close ties to the FBI to examine the servers and provide the evidence to the bureau.

Mr. Comey said the FBI always prefers to examine such devices itself, and that he didn't know why the Democratic officials didn't give the bureau access. Mr. Trump has cited the lack of FBI access to the servers as part of the reason for his skepticism about the spy agencies' conclusions that Russia was behind the hacking.

Write to *Devlin Barrett at devlin.barrett@wsj.com*

EDITOR'S NEWS PICKS

EU To Scrutinize Data Collection: European Union officials proposed new

measures Tuesday that could limit US firms' ability to track EU citizens' personal data without oversight, Ars Technica reported. The European Commission says it plans to tighten the rules around the ePrivacy Directive, which forces communication providers to protect user data and respect confidentiality guidelines. Facebook, Google, and others have largely sidestepped the rules thanks to a distinction that regulates Over-the-Top services differently than telecoms. Now, though, that loophole is likely closing.

Ukrainian Experiments: Russian hackers could be using critical infrastructure in Ukraine as a laboratory for testing the most effective ways to launch a cyberattack, Kim Zetter writes in Motherboard. Investigators say an hour-long power outage in Ukraine at the end of 2016 was the result of malicious activity. That came almost exactly one year after a similar hack turned off the lights for more that 200,000 people in the middle of a cold winter. "They could do many more things, but obviously didn't have this as an intent," one researcher said. "It was more like a demonstration of capabilities."

Lawmakers Question Transit Defense: Sen. Mark Warner, co-founder of the Senate Cybersecurity Caucus, wrote a letter to the Washington Metropolitan Area Transit Authority inquiring about the cybersecurity measures in place there. He asked for details on network segmentation, backup systems, and whether information sharing procedures are in place in the event of a potential cyberattack targeting the D.C. public transportation. The request, surfaced by CyberScoop, comes after ransomware hackers tried to extort $73,000 from the city of San Francisco by holding the subway system hostage.

Easy Security Tips To Remember: One reason effective cybersecurity is so difficult is because there are so many problems that it's hard to know where to start. So journalist Brian Krebs offers a tip sheet full of things every internet user should keep in mind when browsing the web. "If you connect it to the internet, someone will try to hack it," he writes. "If what you put on the internet has value, someone will invest time and effort to steal it." Head to KrebsOnSecurity.com for more truisms.

Invest Less Money, More Time: Believe it or not the best prescription for better security posture might be a company-wide happy hour. Most data breaches start with a human mistake, not a technology flaw, so businesses should communicate with employees on the best way to adopt new technology policies. If a software program is difficult to use, for instance, workers are more likely to take a shortcut, and perhaps rely on a less secure product. Fast Company has more advice on solving organizational annoyances before they become security dilemmas.

WSJ PRO CYBERSECURITY