August 2016

Cyber Security

Special Report

Sponsored by:

RynohLive®
Absolute Financial Protection

Produced by:

THE LEGAL DESCRIPTION

OCTOBER RESEARCH LLC

ABOUT US

The Legal Description is a production of October Research, LLC specializing in business news and analysis for the settlement services industry and is published 24 times a year.

Contact information:
October Research, LLC
ATTN: The Legal Description
3046 Brecksville Road, Suite D
Richfield, OH 44286
Tel: (330) 659-6101
Fax: (330) 659-6102
Email: contactus@octoberresearch.com

TO SUBSCRIBE, PLEASE GO TO
www.OctoberStore.com

OCTOBER RESEARCH LLC
KNOWLEDGE... THE COMPETITIVE ADVANTAGE

EDITOR'S NOTE

THE LEGAL DESCRIPTION

What's a title agency to do?

Dear Readers,

The Internet is a wonderful, but potentially dangerous place. Sometimes it feels like there are landmines dotted across the cyberlandscape that we just can't avoid, ready to take our money and information. Even national governments and political parties aren't immune to data breaches, so what is a title agency to do?

This report is designed to help you answer that specific question. There are resources out there that you might not have thought about to keep ahead of cyberattackers. A massive email hacking scheme has hit our industry hard in the last several months, but if you are able to think through a few specific questions when getting certain, potentially questionable emails, you can stay ahead of the hackers.

Government entities have this on their radar as well and have issued various new laws, regulations and proposals to help protect consumers from cybertheft. We want to help you keep up to date on all of these changes as well.

Thank you to our sponsor of this special report, Rynoh*Live*, for helping us get this education out to our readers.

Until next time, stay legal,

Andrea Golby

Andrea Golby
Editor
agolby@octoberresearch.com

Table of Contents

The more you know: Education as protection against cybertheft

It seems like every day we are hearing about a new threat to our cybersecurity, a new hack that occurred, a new virus that has no cure. Things change quickly in a digital world and as fast as law enforcement and cybersecurity experts work to stop cyberthieves in one area, another area pops up.

Diana Hoffman, vice president, corporate escrow administration, Fidelity National Financial, said during a session at the American Escrow Association's annual conference that cybercrime is up 48 percent and that there are reports of 42.8 million total attacks per day. She noted that in 70 percent of cases, the hackers were able to get in because of some sort of human error.

In a hearing on cybersecurity held by the U.S. House Small Business Committee, **Jamil Jaffer**, director of the Homeland and National Law Program at the George Mason University School of Law, noted in his prepared remarks that in September 2015, **James Clapper**, the director of national intelligence, said that the intelligence community's primary concerns are low to moderate-level cyberattacks from a variety of sources which will continue and probably expand, imposing increased costs to businesses.

In addition, in prepared remarks for that same hearing, **Nova Daly**, senior policy advisor, Wiley Rein LLP, cited a study issued by the Center for Strategic and International Studies in 2013, which estimated that the estimated cost of cybercrime in the United States was approximately $100 billion. Daly said that more recent reports estimate that cybercrime costs have quadrupled since then and are on target to quadruple again between 2015 and 2019.

This makes it all the more critical for title agents to pay attention to news about cybercrime and educate themselves on the latest viruses and how best to combat them.

To give an example of how important education was in the fight against cybertheft, **Matt Lemma**, CIO, certified CISSP, CPHIMS, ITIL and PMP at Rynoh*Live*, pointed out that years ago, people fell victim to chain letters.

"Everyone jokes now, it was so common there for a while," he said. "People are inoculated now to that type of scam because it became mainstream knowledge; very few people respond to chain letters now due to heavy education around that topic."

But now things are more sophisticated. He stressed the criticality of individual learning about different scams and how to avoid falling prey to them. Employees will approach situations differently by understanding how Company X was exploited.

"You learn to apply safeguards and controls that weren't there when something happened to Company X," Lemma said. "This is a continuous learning paradigm requiring full time diligence. Training and security awareness programs are a must to introduce constant learning into the organization."

He said there is lots of information about big hacks, such as Target, and you can look up a kill chain analysis that explains all the steps that were taken. Lemma said that when he gave a presentation earlier this year, he had to make the font size almost unreadable on a PowerPoint slide in order to show all the steps the hackers in the Target hack took. That hack, he said, was a six-month process of basically living on the company's networks and figuring out how to get the magnetic swipe data from Target.

For agents that want to dive further into the threats that are out there, Lemma said he visits Hackers News, a legitimate news site that has lots of information about new zero day viruses (which are viruses with no known fix

yet, ones that are not yet in the signature files of antivirus programs). He said that using that and other security-related websites (e.g. US-CERT, SecurityWeek, OWASP, and CNET security) will provide you with that news more quickly than solution driven sites such as DoD's Security Technology Implementation Guide (STIG) site.

Lemma suggested that part of an agency's risk management process should be a patch management process. He said that when software manufacturers introduce a new patch, they'll inform customers about the new functionality that is included in the patch, but that a lot of times there is an antivirus software update shortly thereafter.

"What is happening behind the scenes is that new security fixes may be driving the upgrade,"he said. "Let's say you installed the next version of Office; now McAfee's signature files need to be upgraded to match that version of Office." This is a very important two-step process which includes new versions and update threat protection files. "Always upgrade to the latest patches to ensure your applications are as secure as possible. This includes shutting down your PC when leaving work for the day so automated network updates can be installed successfully."

He said the STIG, a government site that lists major flaws with IT systems, tools and software, can be helpful. He said a patch management process can be built around STIGs. You can go on a see what the current STIGs are, a description of the vulnerability and a description of a process to address that vulnerability. Lemma said someone from the title agency could go on and look up a particular software or operating system they are using and find out how to address any issues.

Lemma said the Department of Defense site would not cover all programs and suggested agents also check with their products' manufacturer. "Unfortunately, there is no one single place to get all of your security posture information." One advantage of using a Software as a Service company is that they are continuously putting out updates because they are Internet applications housed in the cloud.

"One very large benefit of the cloud is that software and hosting vendors can apply updates and respond to new versions on demand, and and address security vulnerabilities very quickly," he said. "That is a good characteristic to have in your product when you are shopping around for closing or settlement products."

Lemma said agencies also should think about what kind of protective software they need. For instance, a mom-and-pop shop might be better outsourcing to a trusted company to secure their servers, email, backup, etc.

"There are inexpensive hosting options or cloud options that smaller companies can leverage," he said. "When they do that, they can leverage the security of those big companies. So setting up Microsoft 365 [for instance], you pay [a monthly fee] to get Office programs, but in addition to that you are getting all the security that goes along with Office because Microsoft built Office 365 is built upon Microsoft's hosted security foundation."

Who is it? Protecting yourself from email hacks

Over the last several years, words such as phishing have become everyday jargon around the country and in the title industry. People are keeping their eyes out for these kinds of schemes, but what if the email seemingly is coming from a trusted partner?

This new wave of fraud is becoming more commonplace and it's important to understand the new scheme and how to detect it.

The scheme

Diana Hoffman, vice president, corporate escrow administration at Fidelity National Financial, said during a session at the American Escrow Association's annual conference that she first heard about this cybercrime around October 2012, when she read about it happening to a financial brokerage firm. By the end of the year, she heard about it happening for the first time in the title industry.

Since then, the situation only has escalated.

"What we are seeing come through email and what we are getting alerted to in 2016, is a level of malware phishing and a campaign that is unlike any campaign that I've seen before," said **Matt Lemma**, CIO, certified CISSP, CPHIMS, ITIL and PMP of Rynoh*Live*.

The Financial Crimes Enforcement Network (FinCEN) even coined a term for this – Business Email Compromise, defined as a sophisticated scam that targets businesses

that regularly perform wire transfer payments. It is carried out by compromising legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

The scam is becoming so prevalent that the Federal Trade Commission (FTC) and the National Association of Realtors are warning homebuyers about an email and money wiring scam. Hackers have been breaking into some consumers' and real estate professionals' email accounts to get information about upcoming real estate transactions. After figuring out the closing dates, the hacker sends an email to the buyer, posing as the real estate professional or title company. The bogus email says there has been a last-minute change to the wiring instructions, and tells the buyer to wire closing costs to a different account. But it's the scammer's account. If the buyer takes the bait, their bank account could be cleared out in a matter of minutes. Often, that's money the buyer will never see again, the FTC stated.

The FTC's scam alert noted that consumers who receive an email with money wiring instructions should stop and not send any wiring information that way. It stated that title companies and real estate professionals know that email is not a secure way to send financial information. If it's a phishing email, report it to the FTC.

Lemma said this scam is built entirely on the vulnerabilities in virus scans and email spam threat reduction software.

"Because that software is there to defend you, someone who knows how those programs works goes and reverse engineers how to get around email detection and make this more believable of an email," he said. "It gets around the spam box, the filters, any threat protection put in place by your network administrator and entices someone to open the email.

"If it's someone you do business with and it's an email address you know, how willing are you to open an email from a source that you know?" Lemma continued. "These types of attacks are getting much more sophisticated."

Red flags and tips to avoid falling victim

The FTC's scam alert provided some tips to avoid being victims of this scam:

- Don't email financial information. It's not secure.
- If you're giving your financial information on the web, make sure the site is secure. Look for a URL that begins with https (the "s" stands for secure). And, instead of clicking a link in an email to go to an organization's site, look up the real URL and type in the web address yourself.
- Be cautious about opening attachments and downloading files from emails, regardless of who sent them. These files can contain malware that can weaken your computer's security.
- Keep your operating system, browser, and security software up to date.

Though directed at consumers, these tips cam benefit title companies as well. Hoffman reiterated a couple of these and shared some other tips as well.

One of her tips was to simply pick up the phone if something doesn't seem right with the request, sharing examples of when doing so protected the title agency and the hacked real estate agent from losing funds, and when the red flags weren't caught and the agent didn't call.

"Make sure that if you receive wire instructions via email, it's very simple to prevent falling victim to this type of crime, pick up the phone," Hoffman said. "Pick up the phone and call the sender at a trusted number to verify that this information was in fact sent by them and verify the actual account information on there. Look for red flags, make sure you are looking for the red flags: email account slightly tweaked, the change in font, the fact that they may have you sending funds to an account name that has nothing to do with the transaction. You want to look for all of those red flags and make sure you are asking questions so you are not falling victim."

You may want to call if the new wiring instructions are having you send the funds to an entity you do not know the person is associated with. Hoffman said that often, hackers have victims send funds to entities rather than individuals because banks allow entities to withdraw any amount of money they choose from an account, whereas they limit the amount individuals can withdraw to $50,000.

Even simply seeing a different name on the account the person is requesting the money to be sent to also should be a red flag, because hackers often use "money mules" to get funds out of the country. Hoffman shared one experience where they were able to get a hold of the holder of the account, who had no clue that the funds were stolen. Instead, the person believed they were getting funds from a business transaction and sending them along to their fiancé to help the fiancé get into the country so they could get married.

Another thing she said was to look at the email address it is coming from. If you work with the person often, most email programs will show that email address as simply the person's name after a few emails back and forth.

"If you are emailing back and forth with a customer and all of a sudden the email comes up and it has an email address [instead of the name], make sure you

are taking a second, if not third, look at that because it could be an indication to you that a hacker is involved," Hoffman said, noting that it can be hard to tell the subtle differences at a glance.

Hoffman said she also has seen emails come through that had been intercepted by a hacker, who then cut and pasted different information into the email.

"Everything else was identical," she said. "Fortunately they did a bad job of pasting the information, but everything else lined up exactly the same and they intercepted it and put the information on top of it. Look for that stuff, too; if fonts are different, stop and ask why the fonts aren't matching up. It doesn't make any sense in this day and age."

After discovery

There are many things to do, and expect to happen, if you believe you have been hacked.

First, Hoffman said that if you suspect you clicked on something you shouldn't have, call your IT specialist to see what happened and how they can help you address it.

"If you accidentally click on something, don't wait for IT to call you and say you've been hacked, call and say 'Oh my gosh, I did something I'm not sure I'm supposed to do,'" she said. "Ideally, you want to ask first if you should be clicking on that link, but sometimes we are going 20 miles a minute, right? Sometimes things get passed up and if you make the mistake, make sure you report it immediately so if anything has gotten infiltrated, make sure to tell so IT can get to it right away."

She also said that if a customer calls and asks where their wire is, it would be best to drop everything to find out where the money has gone, so as to not lose time in trying to recoup stolen funds.

Hoffman said that if you discover a wire has been sent due to one of these hacks, it's important to contact your bank right away so they can put a recall for fraud and notify the receiving bank and, hopefully, put a freeze on the account.

"In some cases they will, and in some cases they won't without the account holder's authorization," she said. "You have to make sure that you are doing everything you can, going at it in any possible direction that you can."

It also may be important to know the receiving bank will want to know the employee's name who sent the wire, to include if they chose to report the incident to federal authorities since they don't know whether that person was involved or not, Hoffman said.

She also noted that if the money is still in the bank account, the title agent's bank wants the agent to sign an indemnity to them so they can indemnify the receiving bank should the account holder try to sue them.

Small businesses at big risk from foreign cyberthreats

America's 28 million small businesses face unique challenges in the fight against cyberattacks, especially those that come from abroad. During a hearing on the subject by the House Small Business Committee, cybersecurity experts spoke about the growing risk small businesses face from foreign hackers and ways to combat this threat.

These threats come from nation-states, such as Russia, China, Iran and North Korea, but also non-state actors.

"Non-nation state entities also use cyberspace extensively," said **Jamil Jaffer**, director of the Homeland and National Law Program at the George Mason University School of Law, in his prepared testimony. "From organized criminal groups motivated by financial gain and terrorist groups seeking to recruit assets, plan operations or conduct information operations,

to hacktivists motivated by ideology and individual criminals or extremists with capable skills, there is no shortage of non-state actors looking to target Americans and their businesses online.

"In addition to the noting of the now run-of-the-mill online marketplaces on the deep or dark web where illicit goods and information may be transferred, the DNI recently identified an increasing effort by terrorist groups to experiment as they seek to develop more advanced capabilities. Moreover, the increasing use by criminals of ransomware to block user access to their own data, sometimes by encrypting it, is becoming particularly effective and popular tool for extortion for which fewer options for recovery are available is a significant problem for individuals and businesses alike."

Vulnerabilities

Jaffer said that small businesses are sure to be at the forefront of the ongoing technology revolution because of their size and flexibility.

"At the same time, this reliance on high-velocity technological innovation and the creation of new intellectual property underlying the products these small, rapidly growing businesses are bringing to market, means that such companies, perhaps more than other parts of the economy, will be increasingly vulnerable to cyber threats," he said. "In particular, such companies are vulnerable to having the core of their business stolen out from under them: the particular innovations and associated intellectual property that they have developed to give them an edge in the global marketplace. Indeed, given that the primary focus of small business startups is often developing and bringing new, innovative products to market as fast as possible, it would not be surprising if, perhaps more than other companies, small business startups are likely to make security a secondary or tertiary focus."

Justin Zeefe, co-founder and chief strategy officer at Nisos Group, said in his prepared statements that foreign cyberthreats target small businesses for profit because they are seen as the path of least resistance.

"As larger organizations professionalized their defensive and reactive postures to cyberincidents, and as stolen data because less profitable due to a stricter regulatory and law enforcement environment, threat actors — in search of profit — turned their focus to targets which had neither the capacity nor the budget to address cyberthreats. A positive feedback loop ensued, in which threat actors only became more dangerous as they adapted to the increasingly sophisticated target set."

He said that as hackers professionalized and the defensive posture of larger organizations improved dramatically, small businesses failed to adapt.

Jaffer said one of the challenges facing small businesses is making sure their IT infrastructure is up-to-date and that known vulnerabilities are patched.

"In a 2016 report, Cisco reported that a one-day scan identified 115,000 of its own devices running on the Internet, 92 percent of which (106,000 devices) had known vulnerabilities in the software they were running," he said. "Cisco further determined that these devices were running software that had, on average, 26 vulnerabilities and, in some cases, Cisco found that its customers in the financial, healthcare and retail sectors using software more than six years old."

Jaffer cited another Cisco study, its 2015 Security Capabilities Benchmark Study, which found that small and midsize businesses show signs that their defenses against attackers are weaker than their challenges demand.

"Specifically, the Cisco survey found that as compared to 2014, fewer and fewer small and midsize businesses are using web security, mobile security, vulnerability scanning and patching and configuration tools, and that of the small to midsized businesses without an executive responsible for security, nearly one-quarter do not believe their businesses are high-value targets for online criminals," he stated. "Cisco also found, perhaps unsurprisingly, that small and midsize businesses are less likely to have incident response and threat intelligence teams, and that such enterprises use fewer processes than large enterprises to analyze compromises, eliminate the cause of an incident and restore systems to pre-incident levels."

"While large U.S. businesses typically have the means to fund and invest in strong and resilient cybersecurity measures to protect their interests, small businesses generally do not have this luxury," **Nova Daly**, senior policy advisor at Wiley Rein LLP, said in prepared remarks. "They often lack the capabilities and/or the resources to pursue strong, entity-wide cybersecurity protections. Further, small businesses often may not be privy to the kinds of broad, industry-wide threat notifications to which larger companies may be. Often, larger companies have the resources to continually monitor and review threats that may arise from certain technology and supply chains, and at times are contacted by the U.S. government when breaches occur."

Daly also said that despite a report by the House Permanent Select Committee on Intelligence in 2012 regarding counterintelligence and security threats posed by certain telecommunications companies doing

business in the United States, these companies continue to grow, at least in part because small businesses often do not have the funds or capacity to engage other vendors to provide cybersecurity monitoring and reinforcement of their security perimiters.

Industry actions

There are steps the experts said small businesses can take to help address the problems.

Jaffer said that small businesses must get buy-in for the need for cybersecurity at all levels of the company.

"Such buy-in will help drive appropriate resource allocation decisions that may not otherwise be prioritized," he said. "Indeed, Cisco's survey of cybersecurity professionals determined that, regardless of the sophistication or cybersecurity maturity of the organization, the single biggest set of obstacles to adopting advanced security processes and technologies were budget constraints, identified as challenges by 38 (percent to) 48 percent of such professionals."

He also said that small businesses should consider working together within their industries to leverage their buying power for cybersecurity services and take advantage of common services.

In addition, he said small businesses "must find a way to work with the government and with larger businesses to share cyberthreat information in real time, at network speed.

Angela Dingle, president and CEO of Ex Nihilo and chair of the education foundation of Women Impacting Public Policy, said in her prepared statement: "Lack of technical knowledge is not an excuse for failure to comply with basic cybersecurity regulations. While it may be difficult for individuals without a technical background to understand the intricacies of these new guidelines, small businesses need to proactively do the following:

- Understand the scope and impact of changes on the business
- Align organizational policies, practices and procedures to comply
- Empower those with the technical expertise necessary to implement the changes
- Provide adequate training to ensure employees are aware of their responsibilities, and
- Hold individuals accountable for compliance.

"Unless properly managed, information security compliance can be a very costly proposition," she continued. "Companies that do not have a solid understanding of information technology and information security find themselves reacting to an ever-changing sea of regulatory requirements that will be costly to implement."

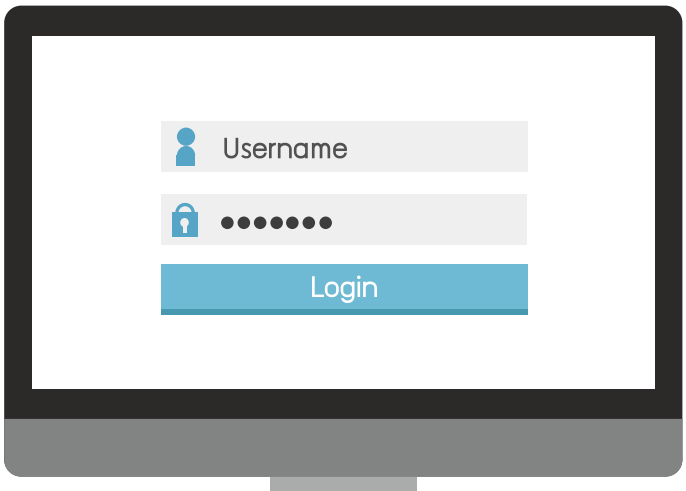
Government actions

There are ways government can help protect small businesses, including getting more serious about deterring nation-state threat actors.

Jaffer called on the government to work to provide more detailed information about the cyberthreats facing the nation to key businesses and political leaders, provide positive incentives to encourage appropriate investment in cybersecurity and information sharing and Congress should consider modifying the Cybersecurity Information Sharing Act of 2015 to provide better incentives for, and remove barriers to, sharing of cyber threat information.

Daly encouraged the committee to consider actions that promote industry-led cybersecurity standards in the framework of ISO standards or best practices.

"Increasing outreach and education to small businesses and finding appropriate funding so that they are aware of the risks to their systems and have the means to address that risk could be pursued," Daly added. "As part of those efforts, it would be useful to strengthen information-sharing initiatives between entities in order to provide small businesses with a more immediate understanding of emerging threats and patterns, and arm these businesses with the lessons learned from others. We could also consider ways to build incentives for purchasing safer equipment. Such market-based cyberincentives, whether in purchasing, insurance or otherwise, would help justify investments in cybersecurity. Profit-minded organizations must see clear benefits to their actions, as every dollar or hour spent on cybersecurity is not spent on the organization's core goals. These actions accompanied with industry norms and standards could highlight cybersecurity investments as requisite."



See.

Rynoh*Live* shows you the fraud and theft risk that lurk just out of sight.

Imagine the convenience and peace of mind you'd have with the ability to see every dollar in every escrow account as it's transferred from one place to another. That's exactly what **Rynoh*Live*** does. It reconciles and electronically verifies your accounts daily to let you see exactly where funds are moving through cyberspace. **Rynoh*Live*** is also the only program that gives your company Best Practice Pillar No. 2 compliance with the American Land Title Association.

Call or visit our website for a free demo and see for yourself what a valuable tool Rynoh*Live* can be.

There is only one.

Rynoh*Live*®

Absolute Financial Protection

877-467-9664 | rynoh.com

Encryption helps keep communication secure

Protecting information doesn't simply mean finding ways to lock down files on a computer or server at your office. It also means keeping the information secure as it's transmitted to and from clients and consumers.

With hackers working to intercept messages and reroute funds in fraud schemes, email encryption has become one of the barriers to protect companies from losing control of sensitive and personally identifying information as they communicate.

RPost CEO **Zafar Khan**, whose company is a leading provider of email encryption, email compliance and cybersecurity software, said those protections are particularly important for title agents. He gave three examples of why encryption should be standard practice in the industry.

"The main drivers of email encryption in the title industry are (1) heightened regulatory enforcement of data privacy rules (note, the recent outsourcing by government regulators of data privacy compliance reviews and audits to private sector enforcers will likely lead to more fines), (2) the potential for cybercriminals to siphon off transaction information and use this knowledge to extract money from the agent, transaction settlement process or consumer, and (3) the potential for cybercriminals to threaten exposure of consumer data under the agent's control while demanding ransom payments," he said. "In short, without email encryption, agent susceptibility to fines and losses increases. With email encryption, there is less E&O exposure."

Time is of the essence, Khan said. He said companies often wait until they have been the victims of a data breach, or have been fined for noncompliance, before seeking an encryption service because they are tempted to defer the investment and not focus on it until something has happened.

"It is important to understand that every unencrypted email sent with consumer non-public information to a consumer recipient is effectively evidence of a compliance breach, residing permanently in the recipient inbox," Khan said. "This notion, combined with the (monetary) government regulator whistleblower awards, incentivizes enterprising or disenfranchised consumers to submit such evidence to the regulators. When title agents pay attention to this, many are quick to realize they should be using email encryption with important consumer email."

So where would you start? Khan said the first question agents need to answer is what information they are sending, and to whom they are sending it.

"For agents, the most important areas to explore are (1) how simple the user experience is for the sender (so it is used) and for the recipient (so they don't complain) and (2) what proof of fact of compliance is returned to the sender organization for use in the event of a data breach," he said. "Additionally, agents should ask to see how well the encryption option sits inside the sender's email program, most often Microsoft Outlook or Gmail."

The threats to unprotected email transmissions continue to grow, and although they might still entail hackers entering a company's system to gain access to logins and passwords they can use for a variety of purposes, Khan said there are other kinds of email attacks as well.

"The greatest cyberthreat in the title sector today is cybercriminals' use of social networking tools and public data to lure participants in the real estate transaction, posing as another participant (title agent, settlement agent, Realtor, buyer, seller, lawyer or lender), into sending downpayment funds to the criminal's bank account," he said. "The FBI reports that millions of dollars have been stolen in the midst of real estate and other transactions with this tactic the tech industry calls 'Whaling' and the FBI calls 'Business Email Compromise.' "

President releases policy directive on cyberincident coordination

The White House has issued a Presidential Policy Directive (PPD) on United States Cyber Incident Coordination, which sets forth the principles governing the federal government's response to any cyberincident. The PPD states that it also establishes lead federal agencies and an architecture for coordinating the broader federal government response for significant cyberincidents. It also requires the Departments of Justice and Homeland Security to maintain updated contact information to help entities that are affected by cyberincidents to report those incidents to the proper authorities.

"United States preparedness efforts have positioned the nation to manage a broad range of threats and hazards effectively," the PPD stated. "Every day, federal law enforcement and those agencies responsible for network defense in the United States manage, respond to, and investigate cyberincidents in order to ensure the security of our information and communications infrastructure. The private sector and government agencies have a shared vital interest in protecting the nation from malicious cyberactivity and managing cyberincidents and their consequences. The nature of cyberspace requires individuals, organizations and the government to all play roles in incident response. Furthermore, effective incident response efforts will help support an open, interoperable, secure and reliable information and communications infrastructure that promotes trade and commerce, strengthens international security, fosters free expression, and reinforces the privacy and security of our citizens. "While the vast majority of cyberincidents can be handled through existing policies, certain cyberincidents that have significant impacts on an entity, our national security or the broader economy require a unique approach to response efforts," it continued. "These significant cyberincidents demand unity of effort within the federal government and especially close coordination between the public and private sectors."

The PPD states that "in carrying out incident response activities for any cyberincident, the federal government will be guided by the following principles:

- **Shared responsibility.** Individuals, the private sector and government agencies have a shared vital interest and complementary roles and responsibilities in protecting the nation from malicious cyberactivity and managing cyberincidents and their consequences.
- **Risk-based response.** The federal government will determine its response actions and the resources it brings to bear based on an assessment of the risks posed to an entity, our national security, foreign relations, the broader economy, public confidence, civil liberties or the public health and safety of the American people.
- **Respecting affected entities.** To the extent permitted under law, federal government responders will safeguard details of the incident, as well as privacy and civil liberties, and sensitive private sector information, and generally will defer to affected entities in notifying other affected private sector entities and the public. In the event a significant federal government interest is served by issuing a public statement concerning an incident, federal responders will coordinate their approach with the affected entities to the extent possible.
- **Unity of governmental effort.** Various government entities possess different roles, responsibilities, authorities, and capabilities that can all be brought to bear on cyberincidents. These efforts must be coordinated to achieve optimal results. Whichever federal agency first becomes aware of a cyberincident will rapidly notify other relevant federal agencies in order to facilitate a unified federal response and ensure that the right combination of agencies responds to a particular incident. State, local, tribal and territorial (SLTT) governments also have responsibilities, authorities, capabilities and resources that can be used to respond to a cyberincident; therefore, the federal government must be prepared to partner with SLTT governments in its cyberincident response efforts. The transnational nature of the Internet and communications infrastructure requires the United States to coordinate with international partners, as appropriate, in managing cyberincidents.
- **Enabling restoration and recovery.** Federal response activities will be conducted in a manner to facilitate restoration and recovery of an entity that has experienced a cyberincident, balancing investigative and national security requirements, public health and safety, and the need to return to normal operations as quickly as possible."

The PPD stated that when responding to a cyberincident, "federal agencies shall undertake three concurrent lines of effort: threat response; asset response; and intelligence support and related activities." In addition, if a federal agency is the affected entity, it shall undertake an additional like of effort to "manage the effects of the cyberincident on its operations, customers and workforce."

This is part of **President Obama**'s Cybersecurity National Action Plan (CNAP), which he unveiled earlier this year to put in place a long-term strategy to enhance cybersecurity

awareness and protections, protect privacy, maintain public safety as well as economic security, and empower Americans to take better control of their digital security.

The CNAP is the capstone of more than seven years of determined effort by the administration, a release from the White House said, building upon lessons learned from cybersecurity trends, threats and intrusions. This plan directs the federal government to take new action now and fosters the conditions required for long-term improvements in our approach to cybersecurity across the federal government, the private sector and the public's personal lives.

As part of the plan, the president is looking to:

- Establish a "Commission on Enhancing National Cybersecurity." This commission will be comprised of top strategic, business and technical thinkers from outside of government – including members to be designated by the bi-partisan Congressional leadership. The commission will make recommendations on actions that can be taken over the next decade to strengthen cybersecurity in both the public and private sectors while protecting privacy; maintaining public safety and economic and national security; fostering discovery and development of new technical solutions; and bolstering partnerships between federal, state and local government and the private sector in the development, promotion and use of cybersecurity technologies, policies and best practices.
- Modernize government IT and transform how the government manages cybersecurity through the proposal of a $3.1 billion Information Technology Modernization Fund, which will enable the retirement, replacement and modernization of legacy IT that is difficult to secure and expensive to maintain, as well as the formation of a new position – the Federal Chief Information Security Officer – to drive these changes across the government.
- Empower Americans to secure their online accounts by moving beyond just passwords and adding an extra layer of security. By judiciously combining a strong password with additional factors, such as a fingerprint or a single-use code delivered in a text message, Americans can make their accounts even more secure. This focus on multi-factor authentication will be central to a new National Cybersecurity Awareness Campaign launched by the National Cyber Security Alliance, designed to arm consumers with simple and actionable information to protect themselves in an increasingly digital world. The National Cyber Security Alliance will partner with leading technology firms such as Google, Facebook, DropBox and Microsoft to make it easier for millions of users to secure their online accounts, and financial services companies such as MasterCard, Visa, PayPal and Venmo that are making transactions more secure. In addition, the federal government will take steps to safeguard personal data in online transactions between citizens and the government, including through a new action plan to drive the federal government's adoption and use of effective identity proofing and strong multi-factor authentication methods and a systematic review of where the federal government can reduce reliance on Social Security numbers as an identifier of citizens.
- Invest more than $19 billion for cybersecurity as part of the president's fiscal year (FY) 2017 budget. This represents a more than 35 percent increase from FY 2016 in overall federal resources for cybersecurity, a necessary investment to secure our nation in the future.

CFPB takes first data security action

The Consumer Financial Protection Bureau took action against online payment platform Dwolla for deceiving consumers about its data security practices and the safety of its online payment system. The CFPB ordered Dwolla to pay a $100,000 penalty and fix its security practices.

Dwolla, Inc., based in Des Moines, Iowa, operates an online payment system. Since December 2009, Dwolla has collected and stored consumers' sensitive personal information and provided a platform for financial transactions. As of May 2015, it had more than 650,000 users and had transferred as much as $5 million per day. For each account, Dwolla collects personal information including the consumer's name, address, date of birth, telephone number, Social Security number, bank account and routing numbers, a password and a unique four-digit PIN.

From December 2010 until 2014, Dwolla claimed to protect consumer data from unauthorized access with "safe" and "secure" transactions. On its website and in communications with consumers, Dwolla claimed its data security practices exceeded industry standards and were Payment Card Industry Data Security Standard compliant. They claimed also that they encrypted all sensitive personal information and that its mobile applications were safe and secure.

But rather than setting "a new precedent for the payments industry" as asserted, the CFPB says that Dwolla's data security practices in fact fell far short of its claims. Specifically, the CFPB found, among other issues, that Dwolla misrepresented its data-security practices by falsely claiming its data security practices exceeded or surpassed industry security standards, and falsely claiming

its information is securely encrypted and stored.

Contrary to its claims, the CFPB said, Dwolla failed to employ reasonable and appropriate measures to protect data obtained from consumers from unauthorized access. Dwolla did not encrypt some sensitive consumer personal information, and released applications to the public before testing whether they were secure.

This is the CFPB's first data security action, and the bureau said it builds off advances made by several other agencies. Under the terms of the order, Dwolla is required to:

- Stop deceiving consumers about the security of its online payment system and enact comprehensive data security measures and policies, including a program of risk assessments and audits;
- Train employees on the company's data security policies and procedures, and on how to protect consumers' sensitive personal information. Dwolla must also fix any security weaknesses found in its web and mobile applications, and securely store and transmit consumer data; and
- Pay a $100,000 penalty to the CFPB's Civil Penalty Fund.

NAIC drafts cybersecurity model law, title industry gives input

A year after the National Association of Insurance Commissioners' Cybersecurity Task Force adopted its regulatory principles, the task force released a preliminary working and discussion draft of a new Cybersecurity Model Law for comment. The American Land Title Association (ALTA) provided its thoughts about how the rule might impact the title industry and small businesses.

The purpose of the proposed model law is to establish exclusive standards for data security and notification of a breach of data security applicable to licensees in the states that would adopt the bill.

Among other things, the model law would require licensees to develop, implement and maintain a comprehensive written information security program that contains administrative, technical and physical safeguards for the protection of personal information. The program would have to be designed to:

- Ensure the security and confidentiality of personal information;
- Protect against any anticipated threats or hazards to the security or integrity of the information; and
- Protect against unauthorized access to or use of the information that could result in substantial harm or inconvenience to any customer.

The scale and scope of a licensee's information security program would have to be appropriate to the size and complexity of the licensee, as well as the nature and scope of the activities of the licensee.

The licensee would have to assess the sufficiency of policies, procedures, personal information systems and other safeguards in place to control identified risks and design and implement information safeguards to control the risks identified in its risk assessment. The licensee would have to regularly assess the effectiveness of the safeguards' key controls, systems and procedures.

The licensee would have to "design its information security program to control the identified risks, commensurate with the sensitivity of the information, as well as the complexity and scope of the licensee's activities, using as a guide, the Framework for Improving Critical Infrastructure Cybersecurity developed by the National Institute of Standards and Technology (NIST), including adopting the following security measures:

- Place access controls on information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing personal information to unauthorized individuals who may seek to obtain this information through fraudulent means;
- Restrict access at physical locations containing personal information, such as buildings, computer facilities, and records storage facilities, to permit access only to authorized individuals;
- Encrypt electronic personal information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access;
- Design procedures to ensure that information system modifications are consistent with the licensee's information security program;
- Utilize multi-factor authentication procedures, segregation of duties, and employee background checks for employees with responsibilities for, or access to, personal information;
- Regularly test or monitor systems and procedures to detect actual and attempted attacks on, or intrusions into, information systems;

- Implement response programs that specify actions to be taken when the licensee suspects or detects that unauthorized individuals have gained access to information systems;
- Implement measures to protect against destruction, loss, or damage of personal information due to potential environmental hazards, such as fire and water damage or technological failures; and
- Develop, implement, and maintain appropriate measures to properly dispose of personal information."

Licensees also would be required to select and retain third-party service providers that are capable of maintaining appropriate safeguards for the personal information at issue.

In its comment letter, ALTA said it appreciated the task force's efforts but asked it to "determine the best approach to protect consumers, whether a state model law would offer a single standard and whether other alternatives could provide consumers with better protections." It also suggested that any potential model law should not duplicate or conflict with existing state law.

"If it is determined that a state model law is the best way to employ a single standard for data security, the NAIC should consider the benefits of beginning the drafting process by hosting an open conversation about data security," ALTA stated. "This open conversation would provide an opportunity for regulators, consumers and industry to identify a shared philosophy and approach to deterring, detecting and preventing cyberfraud. A roundtable of this type will also help licensees (including producers) understand the public policy objectives that NAIC is trying to achieve and how we can reach those shared goals together. A consensus view among regulators, industry and consumer groups about shared goals and objectives for data security will more effectively protect consumers. That consensus, followed by an open, transparent process of review, public comment and approval, will allow us to produce an effective standard for data security and investigation and notification of a breach of data security.

"Without an open, thoughtful and constructive conversation, the Preliminary Working and Discussion Draft runs the risk that its purpose and effect will be neither clear nor transparent, and a subsequent model law is likely not to be adopted by state legislatures," the association continued. "This concern poses a significant risk for state insurance regulators. In addition, if the NAIC were to adopt a subsequent model law, it is possible that many licensees would prefer a state-by-state data security framework rather than this proposed single standard."

States continue amending data breach statutes

As more is learned about data breaches, and the ways in which cyberthieves achieve their goals become more sophisticated, states have had to evaluate and amend their statutes regarding data breaches. This year was no different, as at least two states have continued the trend.

Nebraska

The Nebraska Legislature adopted revisions to the state's Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006.

The bill, **LB 835**, was introduced by Sen. **Heath Mello** of South Omaha.

Under current law, encrypted means "converted by use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without use of a confidential process or key." The new law would clarify that "data shall not be considered encrypted if the confidential process or key was or is reasonably believed to have been acquired as a result of the breach of the security system."

Currently, personal information means a Nebraska resident's first name or first initial and last name in combination with one or more of the following data elements, if either of them are not encrypted, redacted or otherwise unreadable:

- The resident's Social Security number;
- The resident's driver's license or state identification card number;
- Account number or credit or debit card number;
- Unique electronic identification number or routing code; or
- Unique biometric data.

Now residents' usernames and email addresses, in combination with a password or security question and answer, also will be considered personal information.

The bill also states, "If notice of a breach of security of the system is required by [this statute], the individual or commercial entity shall also, not later than the time when notice is provided to the Nebraska resident, provide notice of the breach of security of the system to the state's attorney general."

Tennessee

The Tennessee General Assembly has adopted a bill that will change the time period in which an information holder must disclose a data security breach.The bill, **SB 2005**, was introduced by Sen. **Bill Ketron**, R-Murfreesboro.

The bill states: "Any information holder shall disclose any breach of the security of the system, following discovery or notification of the breach in the security of the data, to any resident of Tennessee whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made immediately, but no later than 14 days from the discovery or notification of the breach, unless a longer period of time is required due to the legitimate needs of law enforcement."

It also will require any information holder that maintains computerized data that includes personal information that the information holder does not own to notify the owner or licensee of the information of any breach of the security of the data within 14 days from when the information holder discovered the breach, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

The notification requirement could be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification then will be required to be made no more than 14 days after the law enforcement agency determines that it will not compromise the investigation.

The act was signed by Gov. **Bill Haslam** on March 24 and took effect July 1, 2016.

Senate committee slated to work on Email Privacy Act

The Senate Judiciary Committee is set to take action on a bill that would amend the Electronic Communications Privacy Act of 1986, after the bill sailed through the House of Representatives by a 419-0 vote.

The House bill has bi-partisan sponsorship in the Senate by Judiciary Committee members **Mike Lee** (R-Utah) and **Patrick Leahy** (D-Vt.). As passed by the House, the Email Privacy Act would:

- Prohibit a provider of remote computing service or electronic communication service to the public from knowingly divulging to a governmental entity the contents of any communication that is in electronic storage or otherwise maintained by the provider, subject to exceptions;
- Revise provisions under which the government may require a provider to disclose the contents of such communications;
- Eliminate the different requirements under current law depending on whether such communications were: (1) stored for fewer than, or more than, 180 days by an electronic communication service; or (2) held by an electronic communication service as opposed to a remote computing service;
- Require the government to obtain a warrant from a court before requiring providers to disclose the content of such communications, regardless of how long the communication has been held in electronic storage;
- Requires a law enforcement agency, within 10 days after receiving the contents of a customer's communication, or a governmental entity, within three days, to provide a customer whose communications were disclosed by the provider a copy of the warrant and a notice that such information was requested by, and supplied to, the government entity; and
- Prohibits disclosure requirements that apply to providers from being construed to limit the government's authority to use an administrative or civil discovery subpoena to require: (1) an originator or recipient of an electronic communication to disclose the contents of such communication, or (2) an entity that provides electronic communication services to its employees or agents to disclose the contents of an electronic communication to or from such employee or agent if the communication is on an electronic communications system owned or operated by the entity.

In introducing the bill before the Senate Judiciary Committee, Leahy thanked Chairman **Chuck Grassley** (R-Iowa) for listing the bill and its unanimous approval by the House.

"The way things have been over there I don't think they would ever have a bill that would say that the sun rises in the East that would pass with that margin," Leahy said. "But we have everybody from the ACLU and Leadership Conference on Civil and Human Rights, to the U.S. Chamber of Commerce and Heritage Action backing it. Either it's a darn good bill or one of them doesn't understand it. But I would hope (this) week (when) we bring that up that we could pass it."

Grassley was cautious about moving too quickly.

"There is some feeling, I don't know if it is among members or outside groups, that since this bill passed the House 400-0 that we should just accept it," he said. "My judgment is the Senate ought to do its due diligence on it. … And so that'll come out next week depending on what sort of bipartisan agreement we can get, if there's going to be any changes. And I'm not anticipating any because I just don't know at this point."

Lee added his support at the bill's listing as well, saying the 30-year-old privacy act was in need of updating.

Senate bill seeks to bolster small business cybersecurity

Sen. **David Vitter** (R-La.), chairman of the Senate Committee on Small Business and Entrepreneurship, and Sen. **Gary Peters** (D-Mich.), introduced the Small Business Cyber Security Improvements Act of 2016, which would enable the U.S. Small Business Administration's (SBA) Small Business Development Centers (SBDC) to work with the U.S. Department of Homeland Security (DHS) to assist small businesses in planning for and protecting against cybersecurity attacks.

The bill would authorize the creation of an SBDC Cyber Strategy through a partnership between SBA and DHS, allowing DHS to provide cybersecurity risk information and other homeland security information to help small businesses develop and enhance their cybersecurity infrastructure, cyberthreat awareness and cybertraining programs for employees.

The legislation also would direct the Comptroller General to conduct a review of current cybersecurity resources of federal agencies aimed at assisting small businesses with developing or enhancing cybersecurity infrastructure, cyberthreat awareness and cybertraining programs for employees. Following the review, the SBA and DHS will work with SBDCs to formulate a plan to address cybersecurity concerns for small businesses.

"Small businesses and entrepreneurs are the backbone of our economy, but cybersecurity attacks pose serious threats to their businesses and their customers," Peters said in a news release. "I am proud to join Sen. Vitter in introducing this bill to provide hardworking Americans with the resources they need to protect their livelihood from cyberthreats. We must help ensure small firms can enhance their cybersecurity infrastructure and preparedness, so that they can continue to focus on creating jobs, spurring innovation, and expanding economic opportunity."

U.S. Reps. **Richard Hanna** (R-N.Y.) and **Derek Kilmer** (D-Wash.) have introduced a companion bill, which currently has 15 bipartisan cosponsors.