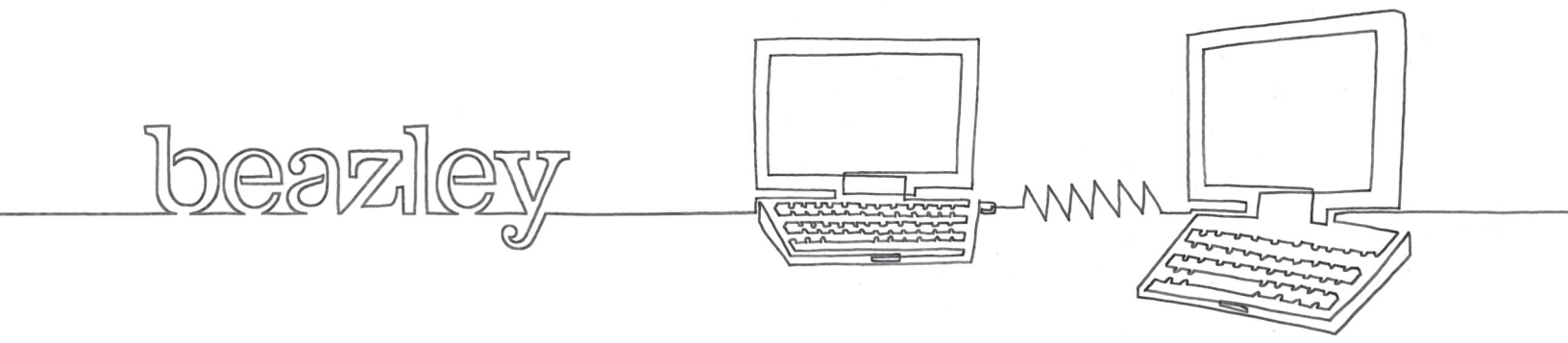
Beazley

2018 Breach Briefing



Contents

Introduction	3
Payroll diversion phishing attacks	4
Cyber extortion	6
Fraudulent wire instruction attacks	8
W-2 email phishing scams	10
Spotlight on retail and hospitality	12
Spotlight on healthcare	13
Conclusion	14
Glossary	15

Introduction

The cyber threat landscape is constantly changing. Malicious attacks like zero-day malware, ransomware, and cleverly targeted phishing attacks are on the rise, but businesses also cannot ignore the all too prevalent accidental disclosures and human error risks. Evolving forms of business interruption, cyber extortion, critical operational data loss, and electronic crime present cumulative risks that businesses must address.

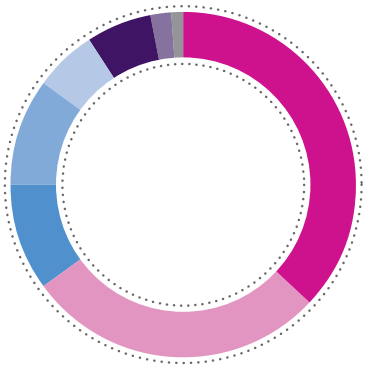
Given the changes in the threat landscape, businesses must protect themselves on all fronts, and a focus on incident response is no longer enough. With Beazley's 360° approach, companies have access to a comprehensive set of solutions created to protect their business from the dangerous world of cyber risks.

Working with our policyholders on over 2,600 data incidents in 2017, Beazley Breach Response (BBR) Services, Beazley's in-house breach response team, has a unique vantage point to see evolving threats first-hand and to directly help with protective measures that organizations can take against these threats. Our 2018 Beazley Breach Briefing provides information on recent key cyber threat trends and useful, proactive steps that organizations can take to minimize these threats.

The Briefing also contains real life examples of each of the threats we describe. We provide these examples so that readers can appreciate and understand not only how these issues actually unfold, but also the services and resources that are required for organizations to diligently investigate and respond to these threats.

As cyber threats evolve, so does the terminology describing these threats. At the end of this Briefing you will find a glossary of key terms to enhance your understanding of the cyber threat landscape.

2017 incidents by cause (total: 2,615)



- Hack or malware 36%
- Accidental disclosure 28%
- Insider 10%
- Social engineering 10%
- Portable device 7%
- Physical loss/non-electronic record 6%
- Unknown/other 2%
- Payment card fraud 1%

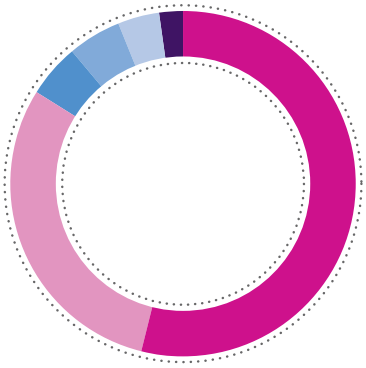
Source: BBR Services 2017

Payroll diversion phishing attacks

In 2017, BBR Services encountered a new variation on the phishing attack: bad actors phish for email credentials, change direct deposit information in employee self-service portals, and then redirect paychecks. If the criminals can also access W-2 information through the payroll processor user account, they may then file a fraudulent tax return for the employee or use the Social Security number (SSN) to open lines of credit.

BBR Services assisted with 54 of these incidents in 2017 across all industries. More than half of these incidents handled by the BBR Services team occurred in the higher education sector, likely due in part to the fact that college and university faculty and staff emails are often publicly listed on school websites. The BBR Services team also handled these incidents in healthcare, manufacturing, professional services, and retail.

2017 payroll diversion phishing attacks by industry



- Education 54%
- Healthcare 30%
- Professional services 5%
- Retail 5%
- Manufacturing 4%
- Unknown/other 2%

Source: BBR Services 2017

Some 84% of payroll diversion phishing attacks reported to Beazley impacted middle market organizations versus small businesses, suggesting larger organizations are more of a target for this type of an attack.

A typical payroll phishing attack happens as follows:

- The attacker targets the organization's employees with an email phishing campaign.
- One or more employees fall for the phishing campaign and supply their email credentials.
- The attacker determines which vendor the organization uses for payroll/HR.
- With the user credentials, the attacker creates a new inbox forwarding rule for the compromised account. The forwarding rule sends any email coming from the payroll provider directly to the trash.
- Using the compromised email address, the attacker requests that the payroll provider reset the password for that account. The payroll provider sends a password reset email with a temporary password. Because of the forwarding rule, the email goes directly to the trash and the user never sees it.
- The attacker uses the newly supplied password to access the employee self-service portal. If the organization uses single sign-on for access to the payroll provider, the attacker doesn't even have to request a password reset.
- The attacker changes the direct deposit information for the employee. The next time payroll is processed, the employee's paycheck goes into an account the attacker controls.

Although BBR Services has seen these attacks primarily compromise direct deposit instructions, the attack can be used on other types of accounts, such as health savings accounts (HSA), flexible spending accounts (FSA), or 401(k)s or 529 plans.

These attacks typically require an external forensic analysis to determine whether the attacker had access to personally identifiable information (PII) or protected health information (PHI) within the employee's email inbox. Employees in some roles, such as a student loan officer in education, loan officer in financial services, or administrator or practitioner in healthcare, may have PII or PHI in emails. If the organization concludes that PHI or PII has been exposed, determining the population of affected individuals can be a time-consuming process that requires extensive mining of emails in order to determine the specific individuals impacted and the exact nature of the exposed PII or PHI.

Payroll diversion phishing attacks *continued*

Phishing attack diverts university's payroll

An attacker targeted a university with a phishing email and gained credentials to 15 faculty email accounts. The university learned of the attack when a few faculty members complained about not receiving paychecks. An internal investigation revealed that the attacker gained access to the user email accounts and used the email credentials to log onto the university's employee self-service portal. BBR Services provided an action plan, including connecting the university with expert legal and forensics services. Notification letters along with an offer for credit monitoring were prepared and sent to the affected persons. Given the states of residency of the affected individuals, no regulators needed to be notified. The forensic firm was also able to rule out the possibility that the attacker viewed the W-2 portion of the portal so the 15 faculty members' W-2s were not accessed. The total cost of this incident, not including the cost of the stolen payroll, was approximately $100,000.

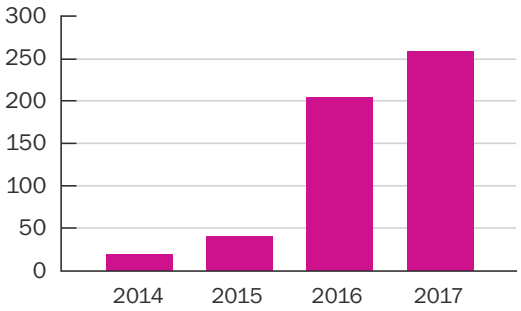
Protecting your organization from phishing attacks

- Turn on two-factor authentication for external access to all applications, or at the very least, to particularly sensitive ones such as email, payroll or benefits providers, remote desktop protocol (RDP), and virtual private networks (VPNs).
- Audit recent direct deposit changes prior to issuing payroll and confirm the changes over the phone or in person with your employees.
- Educate and train employees about phishing. Consider whether simulated anti-phishing campaigns make sense for your organization's risk profile.
- Periodically review email distribution lists, especially where reports containing PII or PHI are sent to a list.
- Use role-based access controls to manage access to sensitive information and ensure that access is terminated or updated appropriately when an employee changes roles or leaves the organization.
- Enforce strong password policies. Educate employees about the risks of recycling passwords for different applications.
- If your email system permits, set up alerts whenever new forwarding rules are created so that messages cannot be secretly diverted.

Cyber extortion

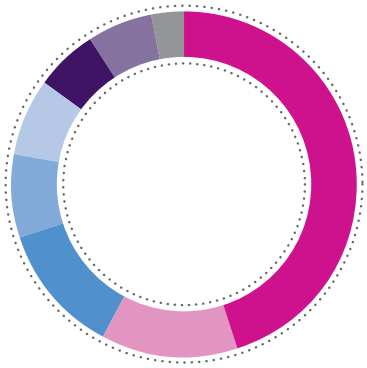
Ransomware remained a constant threat in 2017, including two notable worldwide attacks. BBR Services saw an 18% increase in ransomware incidents in 2017, and ransomware attacks are still occurring across industries and market segments. And while BBR Services received more notifications of ransomware attacks from smaller companies, notifications from larger companies in the middle market still accounted for 42% of the 2017 ransomware attacks notified to Beazley.

The rise of ransomware



Source: BBR Services 2017

2017 ransomware incidents by industry



- Healthcare 45%
- Financial 12%
- Professional services 12%
- Other* 8%
- Manufacturing 7%
- Education 6%
- Retail 6%
- Hospitality 4%

Source: BBR Services 2017
*Includes utilities, construction, government and real estate

Worldwide ransomware attacks

In May 2017, the WannaCry ransomware attack struck 200,000 computers in more than 150 countries. Unlike most ransomware, which spreads when users click on a link in a phishing email, WannaCry included a worm that exploited a vulnerability in unpatched Microsoft operating systems to spread itself very quickly within networks and to external systems that shared the vulnerability. Many overseas entities, in particular hospitals in the UK, were affected. The attack was less severe in the US, but highlighted just how critical timely security patches are.

In June 2017, another worldwide attack, known as NotPetya, made the news. The malware was suspected to be the result of Russia weaponizing an existing version of ransomware for what appears to have been an attack on Ukraine's infrastructure. The attack was initiated by compromising popular Ukrainian banking software MeDoc and including the malicious code in the software's automatic update process. Any organization that does banking in Ukraine likely had this software on their network.

Once it infected an endpoint, NotPetya could spread quickly within the network, and if a company was connected to other companies' systems, it could spread laterally. NotPetya exploited the same vulnerabilities involved in the mostly non-US spread of the WannaCry ransomware in May 2017, but also made use of legitimate Windows administrative tools to propagate itself, so the impact on US-based companies was more significant.

A number of Beazley policyholders reported being hit with NotPetya, and BBR Services worked with them to secure legal counsel and a forensic investigation so they could determine what data was at risk and whether they had legal obligations to notify affected individuals.

Cyber extortion *continued*

Manufacturer extorted

A manufacturer notified BBR Services that it received a ransom email demanding five bitcoins in exchange for not selling employee information. The extortion threat was legitimate, as the attacker provided the names, SSNs and other information for a subset of employees. BBR Services connected the company with expert data breach counsel and recommended that the manufacturer work with a forensic firm that maintains a reserve of bitcoin and has expertise in negotiating and facilitating ransom payments. The forensic firm attempted to negotiate the ransom amount, which bought time to investigate and determine that an employee's inbox had been compromised, and using those credentials, the attackers were able to move throughout the network and ultimately exfiltrate sensitive employee data. Notification letters offering credit monitoring and an internal employee communication plan were prepared. In order to prevent employee information being released on the dark web, a decision was made to pay the ransom and notify approximately 1,000 affected employees. The total cost of the services and ransom payment was over $70,000.

Criminals threaten release of investor data

After an investment firm discovered it was hit with ransomware, BBR Services quickly helped the firm engage expert breach counsel and forensic experts to investigate and communicate with the threat actor. Several of the firm's executives received an email claiming that the threat actor had stolen investor data and demanding a multi-million dollar payment in exchange for not releasing the information online. The forensic investigator found signs of inappropriate access to the network and exfiltration of data prior to the ransomware being installed. The investment firm was faced with notifying its investors and BBR Services arranged crisis management services to assist with investor communications. In addition to emails to the investment firm, the threat actor also contacted individual investors demanding payment in exchange for not releasing their information. After some investors' information appeared on social media and data sharing platforms, counsel assisted the firm in getting the information removed and communicating with the investors the steps they could take to protect themselves. The total cost of the services and ransom payment exceeded $65,000.

Protecting your organization from ransomware attacks

- Train employees on the indicators of ransomware and malware, how to identify phishing emails, and how to report suspected incidents.
- Keep systems up to date and patch as soon as possible. For smaller organizations, enable automated patching for operating systems and browsers.
- Segregate networks based on functionality and the need to access resources, including physical or virtual separation of sensitive information.
- Limit unnecessary lateral communications within the network.
- Manage the use of privileged accounts. Implement the principle of "least privilege." No users should be assigned administrative access unless absolutely needed. Those with a need should only use them when necessary. Limit the use of administrative shares.
- Configure access controls including file, directory, and network share permissions with least privilege in mind. If a user only needs to read specific files, they should not have write access.
- Harden network devices with secure configurations, including disabling unnecessary services and remote administration protocols. Always change default passwords.
- Keep offline data backups up to date. Recent attacks have deleted backups accessible from the network, making it harder to recover your data.
- Take advantage of threat intelligence resources including alerts from US-CERT and information provided by regulators for your industry, such as the Health and Human Services (HHS) Office of Civil Rights Privacy and Security listserv.
- Enforce strong password requirements. Longer is better. Windows systems can be configured to require 14 characters as a minimum.
- Eliminate unused service accounts and monitor which accounts are using remote desktop protocol (RDP). Disable any unrecognized or unauthorized accounts.
- Consider using a product that prevents brute-force attacks using RDP, so that an account is locked after a certain number of failed login attempts.
- Require two-factor authentication for external access to all applications.

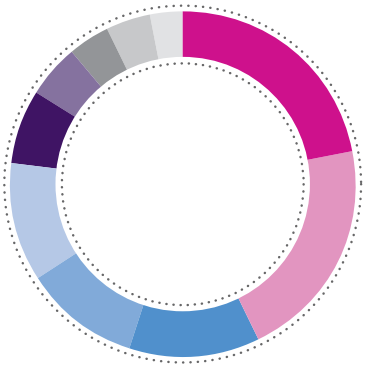
Fraudulent wire instruction

During 2017, BBR Services saw a sharp increase in the number of sophisticated social engineering schemes, frequently taking the form of business email compromises (BEC). In fraudulent instruction attacks, a cybercriminal uses compromised email credentials to induce an employee to make a wire transfer or other electronic payment to a bank account controlled by the cybercriminal. The business email account is first compromised after a successful phishing incident or through installation of a key logger. The criminal can use the access to gain insight into company financial protocols related to wire transfers. Then, the criminal leverages a trusted relationship to provide instructions for the target organization to divert a planned payment or to cause a fraudulent payment to be made. The target of the fraudulent instruction is often a trusted business partner or someone with internal authorization to make wires on behalf of the victim organization. For instance, we often see these incidents occurring in a real estate transaction, where lawyers, real estate agents, and title or escrow companies are frequent targets and the cybercriminal can exploit the short timeframe for the closing to take place. In a recent incident, the cybercriminal compromised a broker's email and sent revised wire transfer instructions, diverting the closing payment.

In another type of BEC scenario, the criminal may not have actually compromised an email account but is able to impersonate a sender the recipient would trust. The apparent sender of an email message can easily be modified, and even with no access to earlier communications between the sender and recipient, a determined criminal may lend credibility to such a "spoofed" message by checking social media for connections, roles, or other supporting details. We also commonly see BEC scenarios where a trusted vendor has itself been compromised. In these cases, the victim organization is the target of the fraudulent wire scheme. For instance, the email account of an employee in the accounting department of a manufacturer was compromised through phishing. The criminal emailed new wire payment instructions to some of the organization's customers. Only after several customers appeared to have missed paying a number of invoices did the manufacturer discover the account compromise.

Victims of fraudulent instruction often lose funds or assets and are also confronted with having to go through a potential data breach analysis to ensure that any email compromise has not impacted PII or PHI.

2017 fraudulent wire instruction incidents by industry



- Professional services 22%
- Financial 21%
- Retail 12%
- Healthcare 11%
- Manufacturing 11%
- Other 7%
- Education 5%
- Hospitality 4%
- Real Estate 4%
- Government 3%

Source: BBR Services 2017

Of the fraudulent instruction incidents reported to BBR Services in 2017, 55% impacted small and medium-sized businesses, and 45% impacted middle market organizations.

Fraudulent wire instruction *continued*

Protecting your organization from fraudulent instruction attacks

- Alert employees who have access to accounts payable systems or wire transfer payments about these scams.
- Train all employees to beware of phishing attempts.
- Establish out-of-band authentication procedures for wire transfer requests and changes to vendor payment instructions. Ensure that confirmation of any instruction involves a separate channel.
- Organizations handling many payments may wish to establish more formal mechanisms for how vendors or customers can change payment instructions, such as implementing app-based two-factor authentication or establishing a preset code.
- Require significant payments, changes to payment instructions, or requests for sensitive employee data to be authorized by more than one employee. Consider a holding period for transactions exceeding a certain amount.
- Turn on two-factor authentication for external access to all applications, but particularly to sensitive ones such as email, payroll or benefits providers, remote desktop protocol (RDP), and virtual private networks (VPNs).
- Enforce strong password policies. Educate employees about the risks of recycling passwords for different applications.

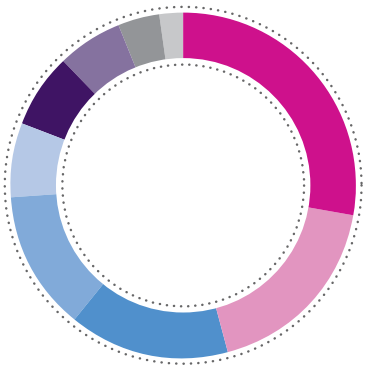
Once an organization becomes aware of potential fraud, time is of the essence:

- Contact your financial institution immediately and request they contact the corresponding financial institution where the fraudulent transfer was sent.
- Contact the Federal Bureau of Investigation (FBI) if the wire is recent. The FBI, working with the US Department of Treasury Financial Crimes Enforcement Network, might be able to help return or freeze the funds.
- File a complaint, regardless of dollar loss: https://www.ic3.gov/ or for BEC/EAC victims at: https://www.bec.ic3.gov.
- When contacting law enforcement or filing a complaint with IC3, it is important to identify the incident as “BEC/EAC.”

W-2 email phishing scams

As BBR Services has seen in prior years, the 2017 tax season saw a large number of W-2 phishing scams. This type of attack involves a threat actor impersonating a high-level person at an organization (typically the CEO or CFO) and acquiring copies of the organization's W-2 forms essentially by duping a human resource or finance department employee into believing the request is legitimate and providing the W-2s to the criminal. The criminal then uses this information to file fraudulent tax returns. Because these attacks focus on tax information, they occur primarily between January, when W-2s are created, and April 15th, at which point the vast majority of individuals have already filed their taxes and the W-2s become less useful to these threat actors.

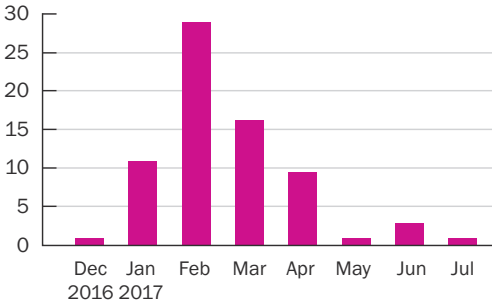
2017 W-2 email phishing scam incidents by industry



- Healthcare 28%
- Education 18%
- Retail 15%
- Professional services 13%
- Hospitality 7%
- Manufacturing 7%
- Financial 6%
- Government 4%
- Other 2%

Source: BBR Services 2017

W-2 email phishing scam incidents by month



Source: BBR Services data year ending 12/2017 (no incidents 9/17 - 12/17)

A distinguishing feature of W-2 phishing incidents is the speed with which criminals use the information. Because they are trying to file tax returns before the incident is discovered – and before the real individuals file their legitimate tax returns – the criminals begin using the W-2 information within days if not hours of obtaining the documents. This means that a victimized organization is also under intense time pressure, with a short window of time to notify its employees and provide them with the information they need to prevent their information from being misused.

This shortened response time makes it necessary to quickly engage expert breach counsel to help draft employee notifications and work with the IRS and credit bureaus to flag the employees' files in order to prevent fraud. Employers need to consider activating a call center and scripting call center agents in order to handle the myriad of questions from upset employees. Because W-2s contain individual and dependents' SSNs, an offer of credit monitoring is recommended for impacted individuals. Adding to this mix is the heightened anxiety faced by employers who ultimately are responsible for allowing the breach of W-2s to occur and are frantic to help reduce the risk of tax fraud facing their impacted coworkers.

Large companies are still falling for this scam

63% of W-2 incidents impacted middle market organizations, whereas 37% impacted small organizations.

W-2 email phishing scams *continued*

Successful W-2 phishing leads to class action against employer

A manufacturing company discovered that one of its employees responded to a spoofed email from the CEO and sent 5,000 W-2s from the previous year to a malicious actor. BBR Services coordinated a speedy response, including quickly arranging expert legal services, notification, and call center services. The notification letters detailed steps the affected employees should take with the IRS and state tax authorities. Despite this quick response, some employees had already fallen victim to fraudulent tax returns. As a result of the breach, the company faced a class action lawsuit filed on behalf of its employees. Breach response costs exceeded $83,000, and do not include defense costs associated with the class action which is still ongoing.

Protecting your organization against W-2 fraud

- Establish clear procedures for how any legitimate request for W-2 information will be handled, and train relevant employees annually on the procedures. If possible, establish a policy that no requests will be made or responded to by email. Policies and procedures should be put in place that trigger a confirmation by phone or other non-email channels before W-2s are sent to anyone.
- Train all employees, especially those with employee payroll or benefits information, to beware of phishing attempts and W-2 fraud.
- Configure your email system to highlight emails coming from outside the network. W-2 phishing emails are often masked to look like they are from within the company, so this defense will call attention to their true nature.

Spotlight on retail and hospitality

In 2017, retail and hospitality companies faced a variety of hacking and malware incidents. Of the hacking/malware incidents managed by BBR Services where forensic services were needed, about half involved a compromise to the e-commerce platform, while the remainder were compromises at the point-of-sale (POS).

Threats to our retail insureds included ransomware, e-commerce compromise, compromise of corporate environment, POS compromises, and phishing of user credentials in order to move throughout environments (then push out card harvesting malware to POS devices).

Point-to-point encryption could have stymied malware attacks

In two of the largest retail breaches reported to Beazley in 2017, the attackers gained access to corporate environments through phishing and moved throughout the corporate and some franchisee networks. The attackers were able to push out malware to POS devices to collect card data from card present transactions. If point-to-point encryption (P2PE) had been implemented properly in these two situations, it is unlikely the card present transactions could have been grabbed by the malware. Thus, the insureds would not be facing PCI assessments if they had implemented P2PE. Though that is not to say the attackers could not have grabbed other sensitive information stored on the networks, such as employee information, rewards/membership information, or cards entered through any e-commerce platforms.

Protecting your organization from credit card attacks

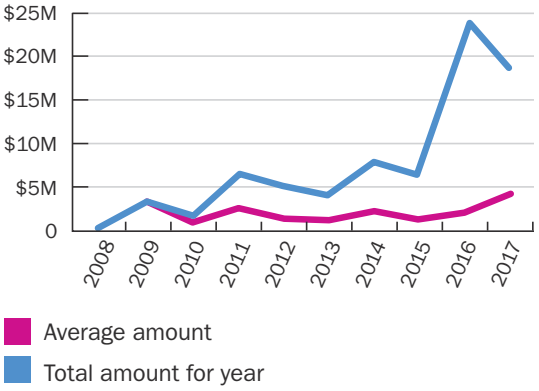
- Properly implement P2PE. The PCI Standards Council has a list of approved PCI P2PE assessors along with a list of approved PCI P2PE solutions.
- Deploy end-to-end encryption software. End-to-end encryption turns payment card data into an indecipherable sequence of characters as soon as the card is read. The data remains encrypted in transit as it is sent across the network to the payment processor. It is readable only by authorized parties that are in possession of the secret decryption key.
- Implement a tokenization solution. Tokenization is a security feature that replaces payment card numbers in transit with “token” values that are meaningless to attackers. A unique token is assigned to each card and stored on a secure server, so the processing system associates a card with its token. Since the card number itself is never sent across the network, tokenization dramatically reduces the risk of compromise. End-to-end encryption and tokenization may be implemented separately, but they provide more robust security when used together.
- Update your POS system hardware to ensure it supports the latest technologies and security features. Similarly, keep POS devices’ operating systems up-to-date by installing patches for security vulnerabilities as soon as they become available and maintain anti-virus software.
- Segment your network so that all POS-related data and computers are on their own isolated segments. That way, even if attackers acquire credentials for your main network, they will not be able to directly access consumer payment card data.
- Purchase POS devices that accept EMV (chip-and-PIN) payment cards.
- Set strong passwords for POS devices. Make sure they are not using default credentials.
- Implement multi-factor authentication (MFA) for remote access to your network. For example, you can require service providers to use a password in addition to another form of authentication, such as a code sent to the cellphone of the person logging in.

Spotlight on healthcare

The Department of HHS for the Office Civil Rights (OCR) heightened its activity in 2017 with nine resolution agreements enforced against healthcare organizations and higher post-breach monetary payments than imposed previously. In 2017, we saw:

- The first resolution agreement for lack of timely breach notification. The covered entity was 41 days past its 60-day window, under the Health Insurance Portability and Accountability Act (HIPAA), with failure to notify affected individuals, the media, and OCR in a timely matter. Also noted is the lag time between the breach, which occurred in 2013, and the resolution agreement, which was announced in January 2017.
- A $5.5 million settlement for failure to review, modify, and/or terminate user's ePHI access. Former employees' login credentials were used to access ePHI for 115,143 individuals.
- A $31,000 resolution agreement for failure of a small for-profit healthcare provider to have a business associate agreement in place with a vendor. The vendor received PHI for approximately 12 years before signing a business associate agreement (BAA).
- The first settlement with a wireless health services provider, for $2.5 million.
- A $2.4 million settlement for disclosing one patient's name to the media.
- A $387,000 resolution agreement for disclosing one patient's HIV status to the patient's employer.

Average and total monetary amounts (including resolution agreements and civil monetary penalties)



Source: www.hhs.gov

Why the increase?

As the chart indicates, the average settlement amounts have increased significantly since 2016. Two reasons for the increase are that OCR has more resources at its disposal and far less patience for HIPAA non-compliance. Settlement payments from resolution agreements are funnelled back into OCR fueling it to pursue enforcement initiatives and increase staffing at regional offices. OCR representatives have also expressed frustration at entities' failure to comply with HIPAA's privacy and security rules, which have been on the books since 2003 and 2005. Hot button issues for OCR include failing to encrypt portable devices, conduct security risk assessments, and enter into business associate agreements with vendors holding PHI.

Protecting your organization from OCR scrutiny

- Regularly train employees on HIPAA and document training.
- Conduct proper risk assessments for all PHI and ePHI.
- Encrypt data at rest and in transit.
- Utilize the minimum necessary PHI when relaying data.
- Notify affected individuals in a timely matter – without unreasonable delay and in no case later than 60 days following the discovery of the breach. This also applies to notifying OCR if the breach affects more than 500 individuals. If fewer than 500 are affected, then disclose in an annual report.
- Ensure BAAs are current, executed, and stored somewhere such that they are easy to locate in the event of an incident or OCR investigation.
- Monitor user credential access to ePHI, and modify as necessary with terminations or changes to position.
- Train employees on email guidance for communications within your organization, with external providers or business associates, and with patients, as well as the use of any encryption solutions you have implemented.
- Institute procedures to double-check patient demographics at visits so information is not sent to outdated locations.
- Train employees about the risks of exposing patient information through the use of social media and the risks of unauthorized access or access beyond the minimum necessary. Audit access to electronic medical records. Audits may include random spot checks across the patient population and monitoring of records of celebrities, VIPs, or other patients who might be of particular interest.

Conclusion

The changing threat landscape

The cyber threat landscape is constantly evolving. The always prevalent phishing attack has morphed into more sophisticated social engineering schemes intended to trick companies into wiring large sums of money or sending employee tax information to criminals. Phishing is being used to compromise email inboxes in order to redirect payroll in employee self-service portals. Cyber extortion continues to plague companies in the form of ransomware attacks, as well as actual instances of extortion where attackers have gained access and exfiltrated highly sensitive data. In the retail context, BBR Services has observed that while P2PE is still the gold standard, it will not prevent all types of hacking and malware attacks. Finally, HIPAA covered entities and business associates face increasingly high settlement amounts as OCR steps up its enforcement activities.

What's on the horizon?

Given the changes in the threat landscape, BBR Services takes a 360° approach to safeguarding against cyber risks and provides Beazley policyholders with risk management, pre- and post-breach services and incident response assistance – all of which are critical to a robust data privacy and security program.

Looking ahead in 2018, cyber events that lead to business interruption are expected to increase. In 2017, the NotPetya malware illustrated the risk of direct damages when it spread quickly from its initial targets, encrypting servers and disrupting corporate networks in Europe and beyond. Manufacturers lost tens of millions when production lines and deliveries were disrupted (forcing cuts to full-year sales forecasts) or shipping and invoicing were delayed. Business interruption from direct attacks is only part of the story. The risk of losses from dependent business interruption continue to increase with the growth of cloud platforms, connected devices, and digitization of supply chains. An interruption in service at a vendor can and will significantly disrupt critical operations.

Compliance with international laws will present challenges for US companies of all sizes. In May 2018, the European Union's (EU) General Data Protection Regulation (GDPR) will be implemented and companies across the globe are preparing. The new protections introduced by the GDPR are not just of academic interest to US-domiciled corporations. The GDPR has extraterritorial impact. For example, non-EU domiciled organizations may fall under the GDPR where they are processing personal data of "data subjects who are in the EU … where the processing activities relate to offering goods or services to data subjects in the EU." This means that US companies with EU-based customers and/or employees may fall within the ambit of GDPR requirements.

The GDPR provides for steep penalties for non-compliance of up to €20 million or 4 percent of global annual revenue, whichever is higher. Under GDPR, organizations are required to notify the relevant supervisory authority, where feasible, within 72 hours of becoming aware of a breach. This creates an almost impossible burden on the affected organization to mobilize resources, respond to an incident, and have relevant experts and partners ready to act. Additionally, the many compliance requirements in the GDPR that are not directly related to data breaches, such as privacy by design and privacy impact assessments, may very well feature prominently in regulatory investigations.

In addition to Europe, Canada is expected to enact/impose national regulations regarding data breach notification in the first half of 2018. In June 2015, Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) established mandatory data breach reporting requirements, but specified that such reporting must be done in accordance with regulations. The PIPEDA provisions will likely require an organization to notify affected Canadians and also the Office of the Privacy Commissioner of Canada (OPC). As with the GDPR and the EU, US companies doing business in Canada or with Canadian citizens may find themselves subject to PIPEDA as it takes effect this year.

BBR Services is uniquely positioned to manage hundreds of data incidents a month across industry sectors. As we expand our global capacity, BBR Services stands ready to help Beazley cyber policyholders face the evolving data and security threats and regulatory landscapes in an informed and well prepared manner.

Glossary

Cybercrime evolves quickly, and so do the terms used to describe it. Here's a guide to some common terms useful in describing the types of risks and incidents we see most often.

BEC (Business email compromise)

A social engineering attack in which a cybercriminal uses compromised email credentials or spoofing to induce an employee to make a wire transfer or other electronic payment to a bank account controlled by the cybercriminal or, in some cases, to transfer sensitive data such as W-2 forms.

Cyber extortion

The threat to encrypt, delete, or release data or to disable a network or website unless a ransom is paid.

Email account takeover

A compromise of email account credentials through phishing or malware that allows a cybercriminal to access an email account and pose as the legitimate owner.

Endpoint

A device connected to a computer network, typically a user desktop, laptop, or server. May also include smartphones or tablets that have access to the network or other devices such as point-of-sale devices or printers.

Fraudulent instruction

A written or electronic instruction intended to mislead the recipient.

Malware

A malicious piece of software or code intended to steal data or credentials, log keystrokes, enable unauthorized access, or otherwise create a risk to the confidentiality, integrity, or availability of data, a network, or other computer resources.

Payroll diversion

A form of theft, often made possible by an email account takeover, in which a cybercriminal changes an employee's direct deposit instructions to redirect a paycheck to an account controlled by the cybercriminal.

Phishing

A form of social engineering in which the attacker, posing as a trusted party, sends an email designed to induce the recipient to share sensitive information such as a username and password, to download malware, or to visit an infected website.

Ransomware

A type of malware used in cyber extortion that encrypts data on an endpoint or network so that the data is unusable unless the victim pays a ransom for the decryption key.

Remote desktop protocol (RDP)

A network protocol that allows a user to establish a connection to a remote computer, often configured for legitimate purposes such as access to an office desktop from home, but easily exploited if not configured properly.

Social engineering

A broad term for techniques attackers use to manipulate someone into providing confidential information (such as login credentials) or taking other actions that bypass normal security and assist the attacker in committing theft or fraud. Social engineering may take place in person (such as getting past a front desk), but the primary means are by phone (for instance, masquerading as tech support) and by email (phishing).

Spoofing

Impersonating a trusted sender, such as another employee, by modifying the apparent source of an email or other electronic communication.

Virtual private network (VPN)

A means to establish a secure connection across a public network as if the connected devices are on the same private network.

W-2 phishing

Phishing directed at employees in the HR, payroll, or finance departments to induce them to send W-2 or other payroll data; most often used to file fraudulent tax returns.

Zero-day

The point at which a hardware or software vulnerability has been discovered, before patches or anti-virus signatures have been developed to reduce the risk of its exploitation.

CBSL500_US_02/18