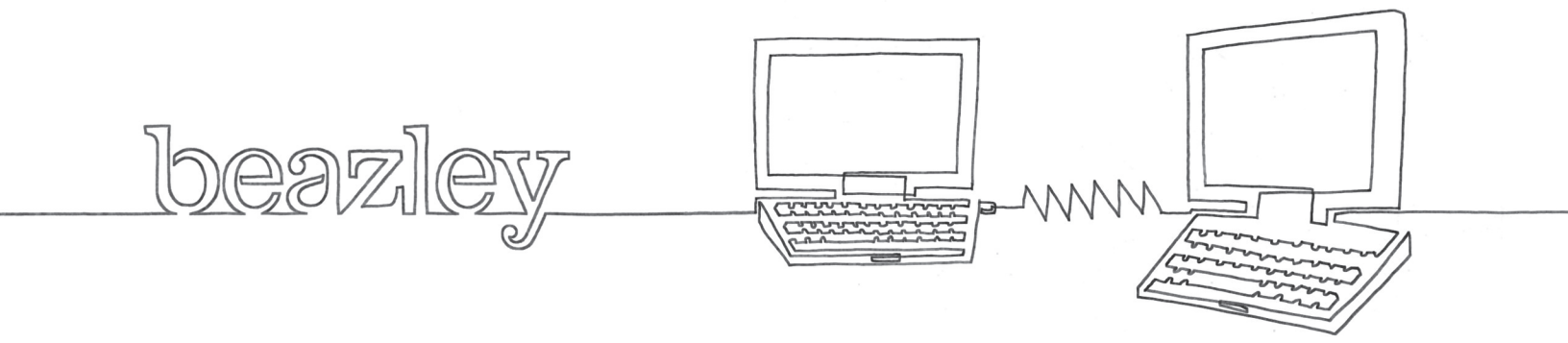
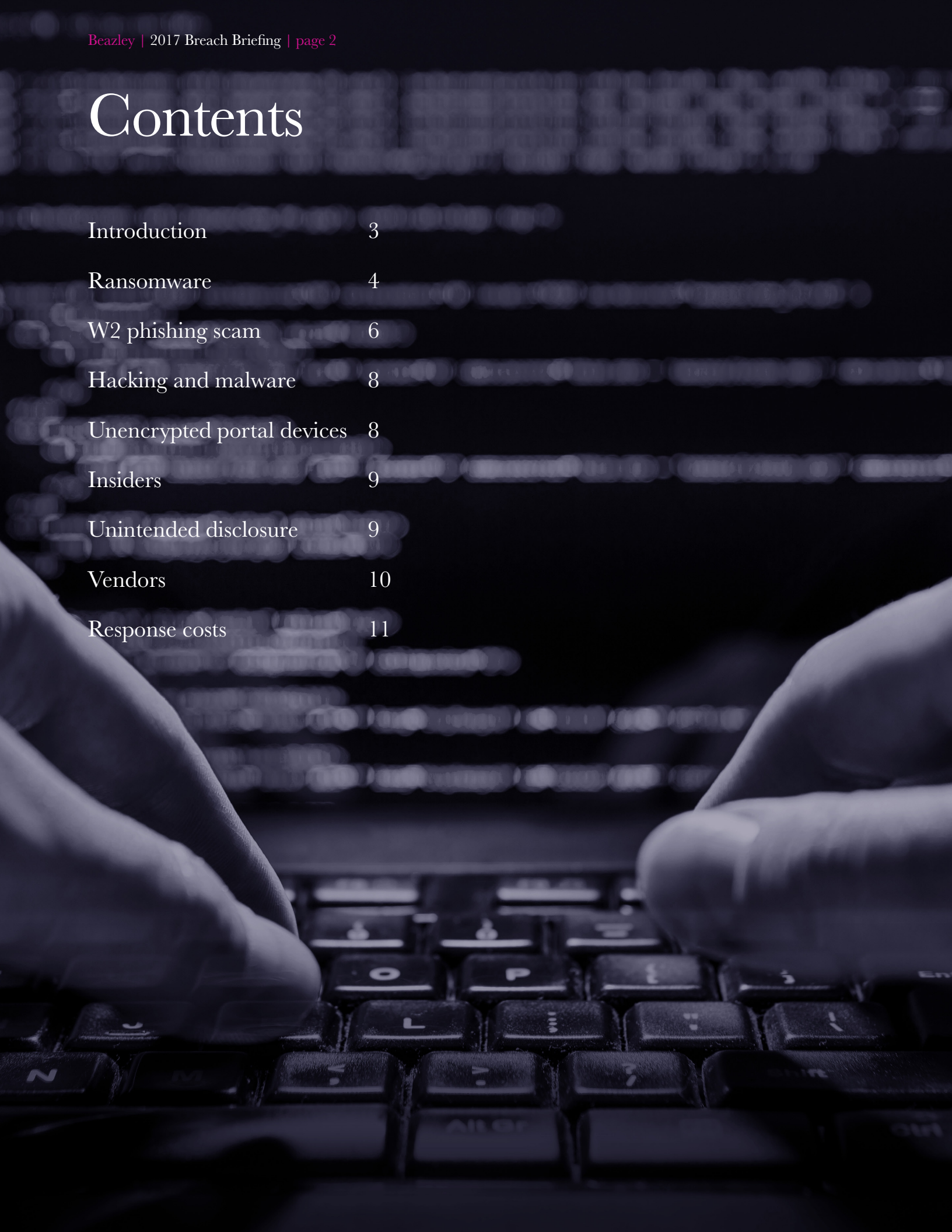
Beazley

2017 Breach Briefing



Contents



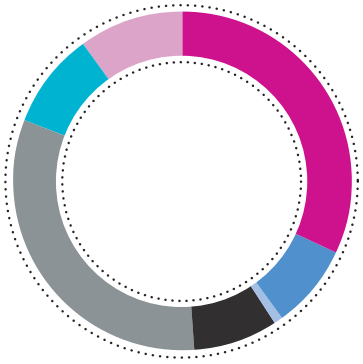
Introduction

At Beazley, we see first-hand the impact of cyber breaches on organizations of all types and sizes. Our Beazley Breach Response (BBR) data breach insurance is backed by our dedicated in-house business unit, BBR Services, which helps policyholders manage the multiple facets of data incident investigation and breach response.

Since the launch of BBR in 2009, we have managed over 6,000 data breaches, nearly 2,000 of which were in 2016. BBR Services is on the front-lines of breach management and has attained a wealth of cyber expertise and knowledge of emerging trends.

From this vantage point we have compiled the 2017 Beazley Breach Briefing, which is based on our 2016 data and provides our unique insight into key trends in data breach causes including factors that impact costs of data breaches.

2016 Incidents by cause (total: 1,943)



- Hack or Malware 32%
- Insider 8%
- Payment card fraud 1%
- Portable device 8%
- Unintended disclosure 32%
- Unknown/other 9%
- Physical loss (non electronic record) 10%

Beazley difference

Beazley is the first and only carrier with a dedicated in-house breach services unit, BBR Services. BBR Services coordinates:

- forensic experts and privacy counsel to help clients establish what data has been compromised, assess responsibility, and issue appropriate notifications;
- mailing and call center vendors to timely notify affected individuals;
- credit or identity monitoring for those whose information is compromised; and
- public relations and crisis management services to help safeguard reputations.

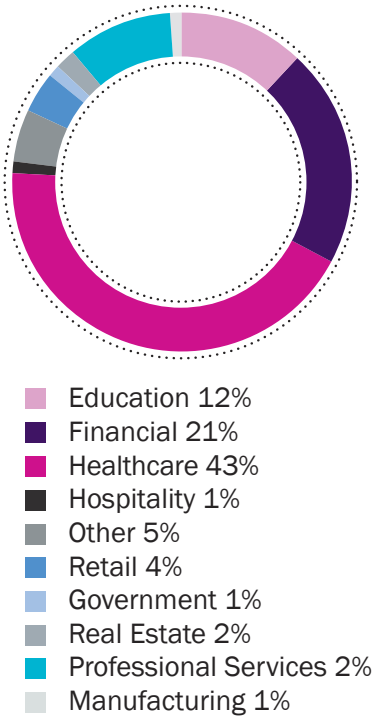
BBR Services also provides risk management resources to help insureds become breach prepared and avoid breaches in the first instance.

Ransomware

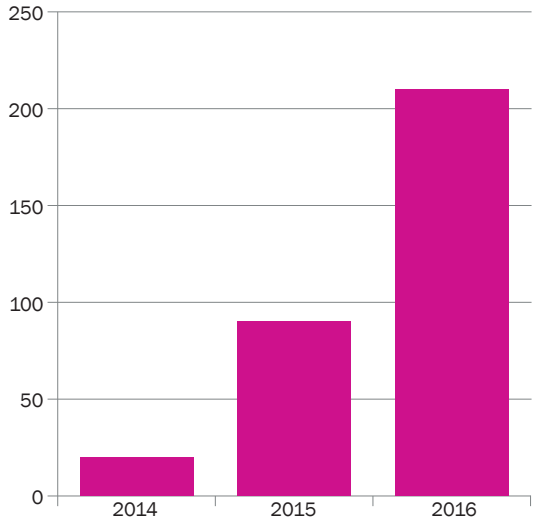
The most significant trend we saw in 2016 was the emergence of ransomware as a key cyber attack weapon. The number of ransomware attacks reported by Beazley insureds quadrupled in 2016 over 2015. No industry escaped ransomware attacks, although Beazley received far more ransomware incident notifications from our healthcare insureds in 2016 than we received from organizations in other industries. The costs of handling a ransomware attack will typically eclipse the costs of the ransom demand, often by a large margin. Additional factors that can increase costs significantly include business interruption and the need to restore lost data post-attack.

Ransomware incidents handled by Beazley (total: 203)

2016 Ransomware Incidents by industry



The rise of ransomware



In a ransomware attack, the perpetrator releases a virus to systematically encrypt files on a system's hard drive, then demands payment of a ransom, usually in a crypto-currency such as Bitcoin, in exchange for the key to decrypt the data. These attacks paralyze businesses, leaving them unable to access the encrypted data unless the data has been backed up and the backups have not also been encrypted by the ransomware virus. Many organizations who receive ransomware demands find themselves considering whether to pay the ransom if they have no other means to regain access to the encrypted data. In managing ransomware incidents, we saw increasing levels of sophistication in attacks. In some attacks, the criminal now goes well beyond merely encrypting data to actually accessing and exfiltrating data. In those attacks, ransomware was launched to mask the fact that the hackers had already taken data out of the system. Another new form of attack exploits the remote desktop protocol (RDP) functionality that is a part of Windows systems. RDP allows a user to establish a connection to a remote computer and is often configured for legitimate purposes, for instance, for an accountant to access his or her office desktop from home. But when users have weak passwords or an organization doesn't monitor service accounts, attackers can use brute force attacks to gain access to accounts with administrator privileges, giving them wide access to the network.

Ransomware *continued*

For a company facing a ransom demand, the questions include:

- Do we have backups of the encrypted data, and if so, how recent are the backups?
- If we have backups, are they also compromised by the ransomware?
- Should we pay the ransom?
- How do we obtain Bitcoin?
- If we pay the ransom, how can we be sure that our data will be released back to us?
- Is the data merely encrypted, or has it been stolen?
- Does the ransomware attack mean we have data breach notification obligations?

BBR Services assists many organizations with these and more ransomware-related questions, including by ensuring that the attacked organization works with experienced legal counsel and external forensics support. Operating hand in hand with legal counsel (under the attorney-client privilege and work product doctrines) forensics experts help determine how the ransomware entered the system and whether it had additional functionality, such as the ability to exfiltrate data. If data was compromised, legal counsel advises on notification obligations.

The stakes of ransomware are now higher for healthcare organizations that are covered entities or business associates under the Health Insurance Portability and Accountability Act (HIPAA). In guidance issued in 2016, the Department of Health and Human Services Office for Civil Rights (OCR) presumes that every ransomware attack encrypting ePHI is a breach and requires a documented analysis, in order to overcome this presumption, that the protected health information was not compromised. This usually means that HIPAA covered healthcare organizations need to incur the expense of professional legal and forensics. If a hospital or health system cannot overcome the breach presumption, notification must be provided to all affected individuals and also to the OCR and to the media if the breach affects more than 500 persons. If fewer then than 500 persons are affected, then notice must be provided to OCR within 60 days of the end of the calendar year in which the breach was discovered.

Beazley cyber extortion and ransomware response services

With thousands of ransomware attacks occurring on a daily basis, ransomware is a threat facing all organizations across all industries. BBR Services provides timely ransomware assistance to BBR policyholders based on our repeated and extensive experience handling ransomware incidents.

If an organization is experiencing a ransomware attack, BBR Services assists by:

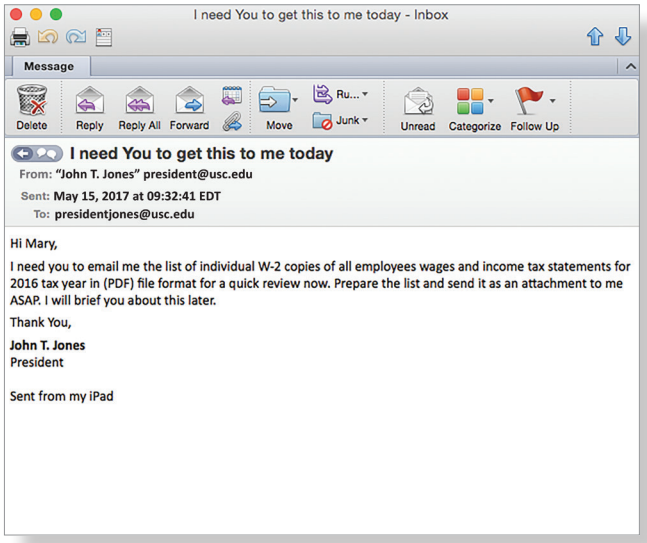
- Promptly consulting with the policyholder to determine an appropriate response;
- Recommending and facilitating a fast connection with computer forensic services to determine if personally identifiable information or protected health information was compromised; and/or
- Facilitating introductions to service providers who can help the policyholder with data decryption, data restoration, or securing bitcoin if their organization decides to pay the ransom.

Hospital under attack

One regional hospital was hit with SamSam – a ransomware strain that comes with particularly high Bitcoin demands. With SamSam attacks, criminals scan for vulnerabilities in JBoss application servers, Java-based web servers, with the publicly available tool JexBoss. If they find a vulnerability, they download an exploit to infect the server. With this foothold established, they look for attached hosts, move laterally through the network, and encrypt those systems. Additional functionality looks for backup files, stops backup processes, and deletes the backup files. BBR Services coordinated the response, lining up privacy counsel, a forensic firm and a crisis management firm. Ultimately, those services cost approximately $70,000, not including the more than 40 Bitcoins paid to obtain a decryption key.

W2 phishing scam

BBR Services saw a marked increase in the number of W-2 email scams, with an increase from only a handful in 2015 up to nearly 70 incidents in 2016. This cyber threat, often occurring but not always confined to the first quarter of the year (before tax day), happens when a fraudster impersonates a trusted party (such as a company executive or trusted vendor) and requests copies of W-2s or employee data that can be used to file fraudulent tax returns. Employers in any industry are susceptible to W-2 fraud via phishing scams. The W-2 incidents reported to Beazley ranged in response costs and have been as high as $150,000.



W-2 breach example

Even the best security controls will not stop an employee trying to be helpful. In one incident, an employee received a spoofed email purportedly from the CEO requesting W-2s and immediately hit reply, attaching all employee W-2s. The company had a restriction on the size of outgoing files, so the email bounced back. The employee emailed the "CEO" (the attacker) to share the bad news, and the attacker helpfully suggested breaking the file up into smaller files and resending. Again, this did not work as the company's email blocked the outgoing message. Frustrated, the employee again emailed the attacker about the failed attempt, and the attacker suggested placing the files up on SharePoint. Once the employee confirmed that she had done so, the attacker stated that he was traveling and couldn't find his SharePoint login, and would the employee be so kind as to give him her credentials. Unfortunately for the employee, and company, she gave out her credentials and the attacker successfully obtained the W-2s of 10,000 employees in the company.

The company began receiving complaints from employees that fraudulent tax returns had been filed on their behalf. After some quick digging, the company learned about what had transpired. The company notified Beazley, and BBR Services connected the company with privacy counsel, a notification and call center services vendor, and credit monitoring.

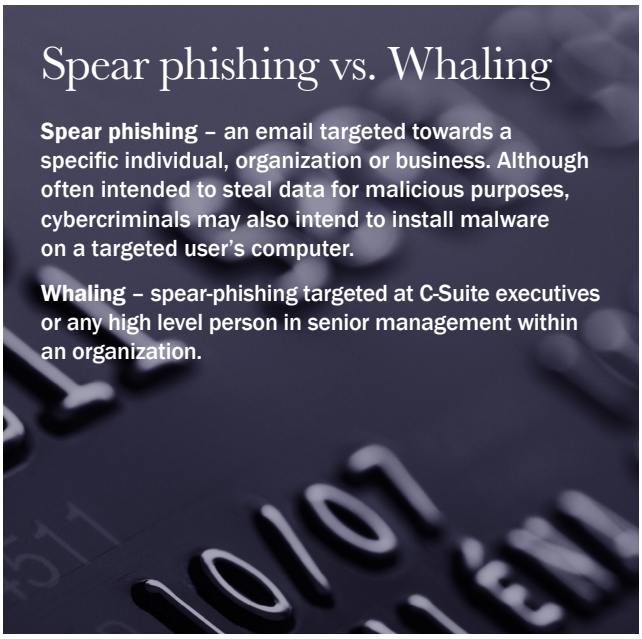
W2 phishing scam *continued*

When employee W-2s are stolen this way, the stakes are very high because employees could be financially harmed by fraudulent tax filings. Indeed, the incident response team tasked with responding to the breach has been personally impacted. The immediate focus is on notifying affected employees and guiding them in contacting the IRS and credit bureaus. Legal experts are marshalled to assist in notifying employees, call centers are set up to handle employee questions, and due the fact that the employee Social Security numbers (SSNs) are included on the stolen W-2s, credit monitoring can be provided to help protect those whose information was compromised.

Spear phishing vs. Whaling

Spear phishing – an email targeted towards a specific individual, organization or business. Although often intended to steal data for malicious purposes, cybercriminals may also intend to install malware on a targeted user's computer.

Whaling – spear-phishing targeted at C-Suite executives or any high level person in senior management within an organization.



How to avoid being a victim of a W-2 attack

To minimize the chance of a successful W-2 attack, here are some steps you can take:

- Out-of-band authentication – After receiving a request for W-2s or other sensitive employee data, employees should be trained to use a separate communications channel to confirm that the request is legitimate before sending the information. Most often, for a request received by email, the employee will make a phone call to a known number to confirm that the person who appears to have made the request did in fact make it.
- Alert employees who have access to employee payroll or benefits information or to accounts payable systems or wire transfer payments about these types of scams.
- Establish clear procedures for wire transfer requests, changes to vendor payment instructions, or requests for employee W-2 or other data, and train relevant employees on the procedures.
- Train all employees to beware of phishing attempts.
- 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.
- Configure your email system to flag incoming and outgoing external email to prevent deception.

Hacking and malware

Hacking and malware is a broad and particularly expensive category of breaches. It can encompass everything from a phishing email that secures system access credentials, to the release of malware that collects and exports credit card numbers via zip files. These incidents typically require the full gamut of response services, from legal servcies, forensics, to notification and credit monitoring, and sometimes crisis management and public relations assistance. These costs add up quickly and BBR Services has seen them climb to over $1.5 million.

32%

of breaches managed by Beazley in 2016 were caused by hacking or malware.

Network attack

An attacker forced its way into a large hospital's network and then proceeded to elevate privileges, moving throughout the network. BBR Services connected the hospital with panel privacy counsel and a forensic firm. The forensic investigation revealed that the attacker could have accessed the entire network, including electronic medical records. After much effort to generate a list of affected patients, the hospital notified approximately 1 million patients with assistance from a BBR Services notification and call center vendor. The hospital also worked with a crisis management firm. In total, the costs of those services were approximately $1.7 million.

Unencrypted portable devices

These breaches happen simply – devices stolen out of cars, a laptop left on a train, for example. But they can involve a complex response, requiring numerous services, including legal, forensics, notification, call center and credit monitoring assistance. Responding to a stolen unencrypted portable device incident can cost hundreds of thousands of dollars. Not reflected in these response costs is the high sum companies may have to pay to regulators, who come down hard on organizations that do not take the relatively simple (and very effective) precaution of full disk encryption on the device. Resolution agreements for the healthcare industry are particularly costly when a lack of encryption is to blame.

Encryption policy fail

A doctor's laptop was stolen in a home break in. Although the laptop was encrypted, the doctor had affixed the username and password to the laptop (against his practice's policy). BBR Services recommended privacy counsel and a forensic firm to investigate what sensitive information may have been on the laptop. Inspection of the contents of the employee's email showed extensive amounts of electronic protected health information (ePHI) and other sensitive information. This information would be available to anyone with possession of the attached credentials. In total, 10,000 patients were impacted and the practice worked with a Beazley mailing and call center to notify affected individuals and offer credit monitoring. In total, the costs of those services were approximately $130,000.

Insiders

There are many ways insiders, malicious or nosy employees, can wreak havoc on an organization – from feeding data to an identity theft ring for profit, to peeking at a celebrity patient's medical records. Unauthorized access to data by insiders can lead to costly and time-consuming audits and forensic expenses to determine the extent of a breach, even before a full response can be marshalled.

Contract employee personal emails

A small bank learned through a routine security audit that a contract employee may have improperly disclosed sensitive information. The contract employee, who was engaged through an agency working on the conversion of the bank's HR system, was sending emails to his personal email account. BBR Services recommended working with privacy counsel and a forensic firm to determine the scope of the compromise. Fortunately, the investigation revealed that there was not a notifiable breach. In total, the costs of those services were approximately $30,000.

Unintended disclosure

Accidents will always happen. An email with protected health information (PHI) or personally identifiable information (PII) is sent to the wrong person. A patient receives someone else's prescription. A mailing goes out with individuals' SSNs in the return address line. The services required to respond to these incidents can vary widely. Forensics costs are often less because the breach is obvious and defined, but notification, call center, and credit monitoring costs can be significant.

40%

of healthcare breaches managed by Beazley in 2016 were due to unintended disclosure.

Publicly available credentials

A university discovered that a page on its website contained an ID and password providing access to the university's administrative site. The administrative site contained data from approximately 70,000 student applicants including SSNs. BBR Services connected the insured with privacy counsel to help determine if notification was required, though a forensic firm was not needed as logging was unavailable. Although the university had no indication that the ID and password were accessed by anyone other than appropriate university staff, there was not enough visibility to rule out access by unauthorized users. BBR Services lined up a notification and call center vendor to notify the 70,000 individuals and offer credit monitoring. The university also worked with a public relations firm. In total, the costs of those services were approximately $110,000.

Vendors

Vendor-caused data breaches are continuing to occur frequently. Consistent with past years, data incidents reported to Beazley in 2016 caused by vendors constituted 13% of the reported data incidents. Beazley sees many reasons why vendors continue to pose problems for their clients and customers including:

- vendors are not put under sufficient pressure by clients and customers to maintain robust security practices;
- vendor contracts are not specific about security obligations and breach notification; and
- vendors, generally speaking, don't care as much about their clients' data as much as their clients do themselves.

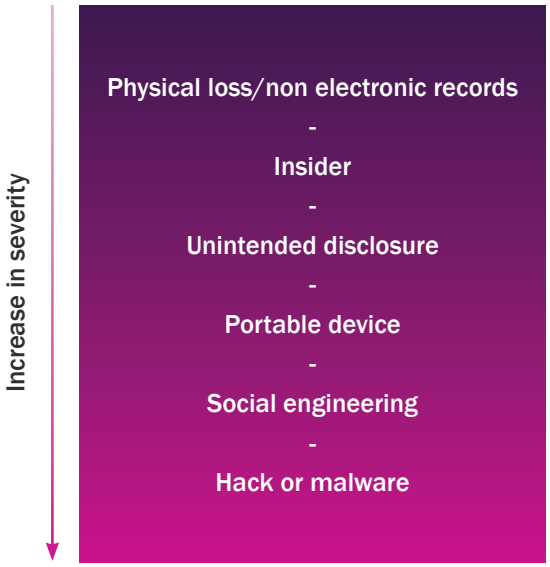
Surprisingly, many organizations still do not realize that their legal obligations to persons affected by a data breach do not go away just because a vendor caused the breach. If a vendor experiences a data breach, depending on a company's contract with the vendor and/or applicable law, the vendor is typically obligated to notify the customer company of the breach in order that the customer company can notify the affected individuals. Beazley routinely sees many variables that impact an organization's legal obligations when a vendor causes the breach, including:

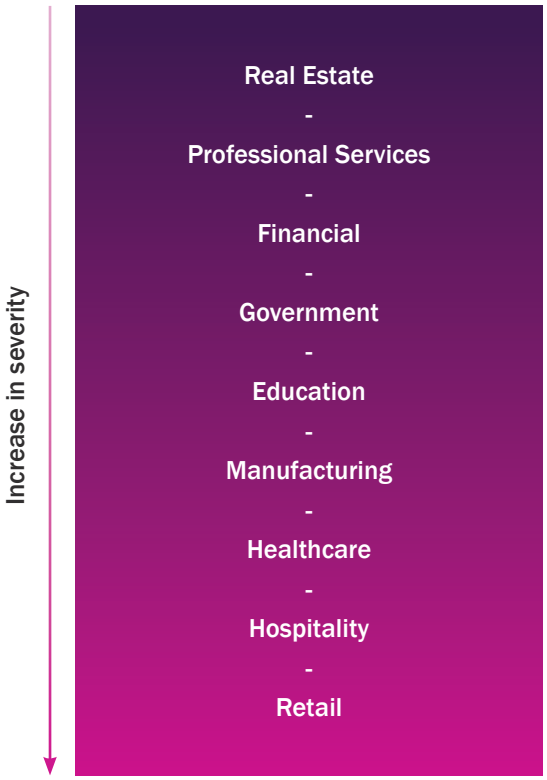
- the vendor's level of cooperation in the investigation;
- the leverage between the parties;
- whether the relationship with the vendor is current versus a past relationship;
- whether the amount of individually identifiable data held by the vendor is appropriate to the current or past vendor services; and
- poorly drafted vendor contracts.

Any one of these variables can make it very difficult for an organization to investigate and respond to a vendor-perpetrated incident. When responding to a vendor breach, BBR Services recommends:

- hiring privacy counsel to advise your company as to its obligations given the information received by the vendor;
- constant follow up with the vendor to ensure the investigation is being handled appropriately (either someone from your company or outside counsel can contact the vendor, though you may get more information if you have someone within the company speaking directly with the vendor);
- determining who will handle notification, call center and credit monitoring (if necessary) – ideally your contract with the vendor already speaks to this; and
- having outside counsel review any notifications that the vendor plans to send affected individuals and regulators (if the vendor is going to take on the notification obligation).

Response costs





A word about data breach costs

The cost of a data breach is something about which organizations with individually identifiable information should care, as the reality of experiencing a data breach is definitely more "when" than "if". However, there are many variables that impact how expensive a data breach can be and meaningful predictors of data breach costs are difficult to state with certainty. Some of our insights on the costs of data breaches:

- The size of a breach is not always a predictor of breach cost. An incident may require no notification as no legal breach occurred, but significant legal and forensic costs were expended to reach that conclusion. By contrast, a W-2 breach requiring notification to 10,000 employees may be less costly despite needing notification, call center and credit monitoring services, because forensics are not needed and attorneys are typically done working on the incident after a few weeks. That said, any breach involving notification to over a million affected individuals will come with significant costs.
- Even small companies can have expensive breaches. For incidents involving forensic investigations, privacy counsel is typically engaged to keep the investigation under the attorney client privilege and work product doctrines. Even if no notification is required, the cost of both legal and forensics will rarely total less than $15,000. More likely than not, the cost to small companies of responding to an incident will cost tens of thousands of dollars, and sometimes hundreds of thousands.
- Other breach costs that can be easily overlooked include the cost of internal time and resources expended on breach investigation and breach response, whether post-breach litigation or regulatory enforcement actions result from a data breach. Reputational damage resulting from a data breach can also be substantial, albeit hard to measure.

In conclusion

From the front lines of helping our insureds with thousands of incident investigations and breach responses across industry verticals, BBR Services continues to share valuable information regarding emerging threats and related risk management actions that companies can take to maximize their security postures and minimize the impact of data breaches.

CBSL500_US_07/17