WHITE PAPER

PROTECTING THE PROTECTOR

EMPOWERING POLICYHOLDERS TO KEEP THEIR BUSINESS DATA SECURE

IDT911

Protecting Identities. Enhancing Reputations.

IDT911 7580 N DOBSON RD, SUITE 201 · SCOTTSDALE, AZ 85256 | PHONE (480) 355 8500 · FAX (480) 355 8501 · WWW.IDT911.COM

1

DATA BREACHES–AND SUBSEQUENT IDENTITY THEFT AND FRAUD–THREATEN BUSINESS POLICYHOLDERS AND THEIR EMPLOYEES AND CUSTOMERS.

What is the value of data stored on company laptops, smartphones and other devices? It's an important question that every business owner needs to consider, especially when these devices contain sensitive customer, employee and institutional information.

In the past decade, more than 860 million records were exposed, and data is more at risk today than ever before.[1] As companies have become more mobile and adopt new technologies, the risk to employee and company data has increased exponentially.

Organizations of every size, in every sector, and in every area of the country are potential targets for a breach. Exposed data can be used for identity theft and financial fraud, or sold on the black market almost as quickly as it's acquired.

Although no two breaches are exactly alike, a common thread is the exposure of personal identifying information (PII), with 33 percent of breaches compromising Social Security numbers (SSNs) and nearly 13 percent exposing credit or debit card information.[2] While it's unknown how many incidents are directly related to device theft, the breach risks from devices are high when you consider how lax many people are with device security. For example, a Consumer Reports survey on personal smartphones found that fewer than half of respondents protected their phone with a PIN or passcode. Only 8 percent had installed software that could erase the phone's contents should it go missing. A full 34 percent took no security measures at all.[3]

Device theft incidents are generally a matter of opportunity. In 2015, thieves grabbed 39 percent of stolen items from a victim's work space, and another 34 percent from an employee-owned vehicle. That said, these items are being lost far more often than they are being stolen. In this year's data, an asset is lost over 100 times more frequently than it is stolen. At the end of the day, the impact is the same.[4] These numbers are all the more frightening when you consider a study conducted by the Ponemon Institute and Intel found that 46 percent of lost laptops held confidential data, and encryption was present on only 30 percent of those devices. Those numbers really hit home, when considering that the average cost of a lost laptop was determined to be more than $49,000, with 80 percent of that figure being attributed to data breach costs.[5] The study also shows that theft and common employee exposures can affect organizations of any size.

1 Data Breaches, Identity Theft Resource Center, May 31, 2016, http://www.idtheftcenter.org/index.php/id-theft/data-breaches.html.
2 Press Release, Identity Theft Resource Center, http://www.idtheftcenter.org/index.php/Press-Releases/breachestop6000.html.
3 "3.1 Million Smartphones Were Stolen in 2013," Consumer Reports, news release, April 17, 2014, http://pressroom.consumerreports.org/pressroom/2014/04/my-entry-1.html.
4 "2016 Data Breach Investigations Report," 44, Verizon.
5 "The Cost of a Lost Laptop," Ponemon Institute, 4, April 22, 2009.

2

INSURANCE COMPANIES CAN PROTECT AND BUILD LOYALTY WITH THEIR BUSINESS POLICYHOLDERS BY OFFERING DATA DEFENSE SERVICES.

For businesses, the damage inflicted by a data breach becomes a long-term realization. Breach response costs build up on top of regulatory fines and penalties, while lawsuits also are often added to the pile.

The total cost of a breach depends largely on the number of records lost, according to the 2015 Verizon Data Breach Investigations Report. Larger organizations, for example, typically have higher breach costs because they lose more records and have higher overall remediation costs.

Expected costs depend on the scope of the breach, ranging between:

- $18,120 - $555,660 for 100 records lost
- $52,260 and $1.5 million for 1,000 records lost
- $150,700 and $74 million for 10 million records lost.[6]

The reputational damage also adds up as people lose trust in the organization and potential customers are put off by the company's presumed lack of security. The financial losses can sometimes threaten the organization's very viability, and brand equity can be damaged for years to come. People want to know that they are doing business with responsible companies that protect their valuable data.

One of the most challenging aspects of a data breach is that lost or stolen information may not ever be made whole again. Even if information from stolen devices is successfully recovered–from a backup file or through manual efforts–the very nature of this sensitive data makes its exposure an event from which full recovery often is impossible. Once an individual's Social Security number, whether it belongs to an employee, contractor, freelancer, or customer, has been exposed or a company's intellectual property taken, there is no way to know who has a copy of it and what they're doing with it.

Even those businesses that aren't breached can be impacted. If one or more employees are affected by an exposure outside the workplace, productivity is likely to drop as a result. Studies have shown that individuals spend an average of eight to 25 hours trying to resolve their identity theft or fraud, oftentimes during business hours.[7]

In a data-driven world that is teeming with devices, how can organizations best protect themselves, their customers and their employees in the event of a breach? Constant vigilance has become essential to ongoing business success. And protection encompasses a range of tools and considerations,

6 "2015 Data Breach Investigations Report," Verizon, 30, 2015.
7 "Identity Fraud: Protecting Vulnerable Populations," Javelin Strategy & Research, 9, 2015.

3

UNDERSTANDING BREACH CAUSES–FROM CYBER CRIME AND EMPLOYEE ERROR TO MORE TRADITIONAL METHODS SUCH AS LOST OR STOLEN DEVICES–IS CRITICAL TO MINIMIZING RISK.

BREACH SCENARIOS

What gets businesses into hot water?

- Missing or stolen laptops or storage devices
- Incorrect mailing or faxing of confidential information
- Erroneous data posting
- Compromised system or network
- Loss or theft of physical documents
- Lost backup data or tape
- Breach caused by third-party vendor
- Improper document/equipment disposal
- Malicious insiders

including smart investments in IT security and information security, as well as in expertise that can help you protect all of your data–especially employee, customer and vendor information.

KNOW THE RISKS

Privacy, cyber and data risks abound in today's environment. A big part of the challenge is that there are so many potential holes in any security strategy. For example, even with robust security measures in place, many businesses can't fully control how, when and where employees use laptops and other devices that may house sensitive data or be connected to the network. Additionally, organizational and individual connections to the online realm are constantly expanding–smartphones and tablets are quickly being joined by smart watches, fitness trackers and other "smart" devices and appliances–and the amount of data flowing across those connections is growing exponentially. This confluence of factors translates into more security holes and potential access points that hackers and cyber thieves can exploit.

A brief recap of highly publicized breaches illustrates the risks. Some of these network intrusions have been nothing short of mammoth in scale. In the retail sector, Target experienced a breach that potentially impacted up to 150 million consumers.[8] That was closely followed by a similar incident at Home Depot that exposed the data of around 56 million consumers.[9] But stores sporting point-of-sale systems that collect payment card information aren't alone in the data breach landscape.

Smaller businesses and organizations also are impacted by breaches. Examples of incidents that regularly occur across the country include:

- A company laptop that turned up in a pawn shop exposed several hundred employee records
- A high-end car dealership break-in resulted in stolen customer information
- A local hospital couldn't locate unencrypted backup tapes
- Confidential records from a local business were found in a Dumpster

These breaches, though they're in different industries and involve different types of data, highlight the enormous danger companies of all sizes face. Organizations in every market sector manage data that is valuable and

8 "$10 Million Settlement in Target Breach Gets Preliminary Approval," *New York Times*, March 19, 2015, http://www.nytimes.com/2015/03/20/business/target-settlement-on-data-breach.html?_r=0.
9 "Home Depot Says Data From 56 Million Cards Taken," *New York Times*, September 18, 2014, http://bits.blogs.nytimes.com/2014/09/18/home-depot-says-data-from-56-million-cards-taken-in-breach/.

4

BUSINESS POLICYHOLDERS CAN MINIMIZE RISK BY CONDUCTING AN AUDIT OF THEIR DATA ASSETS, ELIMINATING UNNECESSARY DATA, AND IDENTIFYING WHICH DATA SETS NEED THE MOST PROTECTION.

highly sought after by thieves. In some cases that's financial data, which may include credit and debit card numbers, bank account numbers, routing numbers, retirement savings plans (401K and IRA), and other important account numbers. In other instances, the information sought by hackers may be more personal in nature. Social Security numbers are routinely stored not only by employers, but also by companies that extend credit or run background checks, such as mortgage representatives, temporary employment services, car dealers, apartment complexes, and many other types of businesses.

Even if a corporate entity isn't hacked, individuals have shown they're surprisingly adept at compromising their own personal data all by themselves. A stolen credit card often ranks as a simple annoyance–call the card issuer, get it canceled–but a lost mobile device could be a real disaster. Stuffed full of stored login credentials, prescription refill numbers, financial account information, and passwords, even the smartphone could expose a person to identity theft if it falls into the wrong hands or isn't properly password-protected against unauthorized access. More traditional risks still exist, as well. A home or business break-in, where thieves are able to abscond with bank statements and other highly sensitive documents, can be a calamity.

MINIMIZE THE RISKS

Fortunately, there are steps businesses can take to help avoid a breach. The approach isn't complex. In fact, it's straightforward and affordable:

Know your data. It's nearly impossible to secure information unless you know where it comes from, where it's stored, and who has access to it. A simple audit of your company's data assets can provide your team with the knowledge necessary to mitigate many existing breach risks. Remember that sensitive information may be in digital or hard copy format, so be sure to thoroughly review all online and traditional data storage locations.

Limit the amount of data gathered and stored. Your company can significantly improve its security posture by eliminating unnecessary data. If you destroy it, hackers can't attack it. Retain only the information required for business operations and securely remove or destroy the rest. Regularly cull obsolete data to minimize privacy risks.

Deploy the right protection for each type of information. With your data audit in hand, determine which data sets are the most sensitive. Those should be given the highest level of protection, while less expensive measures can be used to safeguard lower-valued information.

5

INSURANCE COMPANIES THAT OFFER IDENTITY MANAGEMENT SERVICES AND DATA BREACH PROTECTION CAN STRENGTHEN THEIR BRAND AND TRUST WITH BUSINESS POLICYHOLDERS AND ENHANCE THEIR REVENUE POTENTIAL.

Employees also can take steps to protect themselves from identity theft and fraud. Encourage them to establish strong passwords for their mobile devices as well as their online accounts, and remind them to use unique passwords for each site and system. In addition, employees should check their credit reports regularly. This enables them to quickly spot potential fraud or suspicious activities.

Prevention 101: Essential IT steps for every organization

- **Password-Protect Devices Used By Employees and Third Parties.** Use strong passwords that contain letters, numbers and special characters. Avoid using the same password on multiple devices/accounts.
- **Maintain Anti-Virus and Anti-Malware Software.** Install and regularly update adequate security software on all electronic devices.
- **Keep Browsers Updated.** Internet browsers regularly release new versions in order to enhance the user experience and to combat known security threats. Always update when a new version becomes available.
- **Back Up Data.** Almost half of all breaches are due to lost or stolen devices. Regularly backup sensitive information and, depending on the data saved, make sure it is in an encrypted state.
- **Power Down.** Encourage employees to power down computers when not in use. Powered off, computers are not accessible or susceptible to attacks or intrusions from the internet.
- **Remove Stored Data Before Disposal.** Before disposing of or recycling any device, remove all files and storage drives. Do not rely on the “delete” function to remove files containing sensitive information.
- **Enable Firewalls.** This will help prevent intruders from entering company networks and accessing devices without authorization.
- **Always Use Encryption and Wi-Fi Protected Access (WPA) to Secure Networks.** Many new systems are using WPA2 PSK (AES) or WPA2 PSK (TKIP), which are more ideal than the use of Wired Equivalency Privacy.

6

IN THE EVENT OF A BREACH, REACH OUT TO EXPERTS THAT CAN GUIDE YOU THROUGH BEST PRACTICES TO HELP MINIMIZE DAMAGES.

KNOW HOW TO REACT IN THE EVENT OF A BREACH

If a breach does occur, organizations need to quickly take the following actions to help minimize damages. In most cases, working with a company that provides consultation and resolution services for security breaches will ensure a much more efficient and effective response than what can be achieved by internal teams alone.

Identify and stop the leak. Powering down network equipment or entire systems may be a tempting option, but that can sometimes make it difficult to conduct a thorough and effective investigation later. Instead, the business should work to find the security weakness and remove access to the compromised areas. That may mean taking a server or an entire system offline.

Determine the scope of the breach. Have instances of malware or other threats expanded from the primary system into other areas of the network? Was only a subset of records exposed? What kind of information was exposed? Employee information, customer records? Your team needs to confirm where the intrusion occurred and how far it extended.

Notify the affected parties. Whether it was employee files or consumer data that was exposed, your organization must alert the victims to the situation. Provide as much detail as you can, but present only the facts you know. Work with your organization's breach response consultants and the involved law enforcement agencies to ensure the information provided to victims doesn't compromise any active investigation.

Develop and deploy a strategy to address the original vulnerability. Before your company can return to normal operations, it's imperative that the security issue behind the breach be completely resolved and the integrity of the network confirmed.

HELP IS AVAILABLE

Fortunately, there are support services available for organizations that experience or suspect a data breach or system intrusion. Experienced forensic investigators can review the situation and work with the impacted company to identify vulnerabilities and deploy measures designed to return the network to a secure state. Specialists also are available to assist in notifying parties who may be affected by the exposure and help the organization navigate compliance issues that may need to be resolved with the various regulatory agencies.

7

EDUCATE YOUR POLICYHOLDERS ABOUT THE THREAT OF A BREACH AND PROVIDE ACCESS TO SPECIALISTS THAT CAN HELP PROTECT THEIR VALUABLE CUSTOMER.

In the event an employee suspects his personal data has been compromised, organizations can provide employees with the tools and resources necessary to address the situation. Identity management services are available to help investigate fraudulent activity and resolve cases of identity theft. Fraud specialists can work with affected employees to: secure credit files; restore tampered financial, medical or other records to their original states; help replace important documents; and work with law enforcement agencies to determine what happened and where concerns may still remain.

INCREASE REVENUE

Offering your business policyholders identity management services is an excellent way to increase revenue potential. Data defense services should be top of mind for every business and organization today, at a time when breaches are rampant and individuals are increasingly worried about the safety of their personal information. Because it's an issue on the minds of many–and because both businesses and consumers are aware of the financial harm, emotional toll, and reputational damage an exposure may inflict–being able to offer meaningful support is good for your business policyholders and their employees.

By providing your policyholders with resources that include identity resolution and access to fraud experts, you're differentiating your services as a trusted adviser and a business partner. You're also empowering business policyholders to pursue a better security posture and reduce breach risks.

CONCLUSION

Fortunately, there are comprehensive services that can help your policyholders understand, prepare for, and respond to a breach or system intrusion. Experienced forensic investigators can review the situation and work with businesses or organizations to identify vulnerabilities and deploy measures designed to return the network to a secure state. Specialists also are available to assist in notifying parties that may be affected by the exposure and help organizations navigate compliance issues that may need to be resolved with the various regulatory agencies. ■