Cybersecurity in the Golden State

How California Businesses Can Protect Against and Respond to Malware, Data Breaches and Other Cyberincidents

February 2014

Kamala D. Harris, Attorney General
California Department of Justice

California Chamber of Commerce
Lookout

Cybersecurity in the Golden State

How California Businesses Can Protect Against and Respond to Malware, Data Breaches and Other Cyberincidents

February 2014

Kamala D. Harris, Attorney General
California Department of Justice

Lookout

CalChamber

Privacy Enforcement and Protection Unit
California Department of Justice
www.oag.ca.gov/privacy

Table of Contents

Message from the Attorney General

California is at the center of the digital revolution that is changing the world. Because of work done by companies right here in our home state, we are more connected – and empowered – than ever before. But we are also increasingly vulnerable, a fact underscored by the recent holiday-period data breaches that impacted millions across the country. Unfortunately, cybercrime, data breaches, theft of proprietary information, hacking and malware incidents are now routine.

Cybersecurity is not a new concern. In 2003, California became the first state in the country to require data breach notifications. And as of 2012, companies and government agencies subject to California law have been required to submit copies of their data breach notices to the Attorney General if the breach involves more than 500 Californians. That first year, we received reports of 131 data breaches, which our office reviewed and analyzed in the 2012 Attorney General Breach Report.[1] This Report, and other studies, have repeatedly shown that cybercrime is largely opportunistic.[2] In other words, the organizations and individuals who engage in hacking, malware, and data breach crimes are mostly looking for "low-hanging fruit" — today's equivalent of someone who forgets to lock her car door. And, in part because of the close connection between the data collected by websites or mobile apps and cybersecurity concerns, our Privacy Unit has published recommendations on aspects of privacy policy statements: *Privacy on the Go, Recommendations for the Mobile Ecosystem* and the California Office of Privacy Protection's *Recommended Practices on California Information-Sharing Disclosures and Privacy Policy Statements*, both of which are available in the Business Resources section of the Attorney General's Privacy web site at *www.oag.ca.gov/privacy*.

Notably, the skyrocketing number of mobile devices has spawned new threats. Many of us now carry devices in our pockets that are more sophisticated than we ever could have imagined just a decade ago. Downloadable applications can render us vulnerable to fraud, theft, and other privacy concerns and mobile devices that are constantly connected to the Internet or local Wi-Fi networks face persistent security issues. Mobile security is an issue that must be on our radar screens as we move into 2014.

I recognize that for many of us, computer technology and cybersecurity are complicated. But there are specific and straightforward steps that all small businesses can and should

take to reduce their risk, as well as effective measures businesses can take to respond to cyberincidents should they take place. This Guide sets forth in plain language a few steps that any business can take to help protect itself, with a focus on small to mid-sized businesses that lack the resources to hire full-time cybersecurity personnel. These firms are particularly vulnerable. In 2012, 50% of all targeted attacks were aimed at businesses with fewer than 2,500 employees. And more significantly, businesses with fewer than 250 employees were the target of 31% of all cyberattacks.[3]

In developing these recommendations, we worked closely with security experts at Lookout, a leading mobile security company, as well as the California Chamber of Commerce. We appreciate their contributions and commitment to addressing the challenging task of preventing fraud and fighting cybercrime.

As the state's top law enforcement official, I am committed to protecting the safety, welfare, and privacy of our people and businesses. I hope this Guide will be a useful tool for all of California's business owners as they continue to contribute to the prosperity of this great state.

Sincerely,

Attorney General Kamala D. Harris

Executive Summary

Relatively small investments in cybersecurity preparedness can yield significant risk reductions. Every business in California should follow the steps summarized below, and discussed in greater length throughout this Guide, in order to reduce the chance they will be a victim of cybercrime. These measures, however, cannot guarantee that businesses will avoid cybersecurity incidents, and the Guide therefore contains recommendations for how to prepare an effective cybersecurity incident response plan.

1. Assume You're a Target

Small size and relative anonymity no longer ensure that you will be left alone. Any company, whether big or small, can be the victim of cybercrime. Just as it has become second nature for most of us to lock our front doors when we leave the house, assume you are a potential target and take basic precautions to protect yourself and your company.

2. Lead by Example

Successful cybersecurity measures require the leadership and dedication of business owners. Cybersecurity is not simply the domain of the "IT person"; executive management has to get involved. Small business owners are uniquely positioned to ensure that they and their employees are following good cybersecurity practices. They are also in the best position to understand their company's network and all the devices that connect to it. This requires dedicating the time and resources necessary to ensure the safety and security of their information assets.

3. Map Your Data

To effectively protect your data, you first need to know the types of data you have and the location of that data. Comprehensively review the data you have stored on your IT systems, both on site and off, and with third parties (include backup storage and cloud computing solutions in your data mapping project). Once you know what data you have and where it is, take a hard look and get rid of what you don't really need.

4. Encrypt Your Data

Encrypt the data you need to keep. Encryption is an important step you can take to protect the data you have on your systems. In basic terms, encrypting data – whether it's email, photographs, memos or any other type of electronically-stored information – encodes it so that those without the encryption keys cannot read it. Strong encryption technology is now commonly available for free, and it is easy to use. The great advantage to encrypting your data is that it renders it far less susceptible to hacking. Finally, machines that handle sensitive information like payroll or point of sale (POS) functions should ideally be on networks or systems separate from machines involved with routine services, like updating Facebook and checking email.

5. Bank Securely

It is essential that small business owners put security first when they engage in online banking. This means that online banking should only be performed using a secure browser connection (indicated by "https" and/or a lock visible in the address bar or in the lower right corner of your web browser window). Online banking sessions should be conducted in the private mode of your web browser and you should erase your web browser cache, temporary Internet files, cookies, and history afterwards so that if your system is compromised that information will not be accessible to cybercriminals. In addition, take advantage of the security options offered by your financial institution. Examples include using two-factor authentication to access your account, requiring two authorized individuals to sign off on every transfer of funds, and setting up account notifications by email or text message when certain higher-risk activities occur on your account.

Also, we recommend setting limits on wire transfers. Sophisticated transnational criminal organizations are now routinely hacking businesses' computers and wiring large sums overseas where they cannot be recovered. To prevent this, set limits on the amount that can be wired from your accounts, and (depending on your business needs) consider asking your bank to require two executive team signatures before sending wire transfers overseas.

6. Defend Yourself

In choosing security solutions, guard against single points of failure in any specific technology or protection method. This should include the deployment of regularly updated firewalls,

antivirus, and other internet security solutions that span all digital devices, from desktop computers, to smartphones, to tablets. Devices connected to your network should be secured by multiple layers of defensive technologies that include, but are not limited to, antivirus technology. Seek out comprehensive security solutions that approach security from multiple perspectives so that you are able to manage risk from the full spectrum of threats you may encounter. Useful capabilities include the ability to remotely locate or wipe a device that's gone missing and the ability to identify and block never seen before attacks using technologies that analyze behavior and/or employ virtualization tools.

7. Educate Employees

Raise employees' awareness about the risks of cyberthreats, mechanisms for mitigating the risk, and the value of your businesses' intellectual property and data. Your employees are the first line of defense, and good security training and procedures can reduce the risk of accidental data loss and other insider risks.

8. Be Password Wise

Change any default username or passwords for computers, printers, routers, smartphones, or other devices. ANYTHING is better than the default. Specifically, you should use strong passwords and don't let your Internet browser remember your passwords.

9. Operate Securely

Keep your systems secure by using layered security defenses and keeping all operating systems and software up to date. Don't install software you did not specifically seek out and don't download software from untrusted or unknown sources. Also remember to remove or uninstall software you are no longer using.

10. Plan for the Worst

Every small business should put together a disaster recovery plan so that when a Cyberincident happens, your resources are used wisely and efficiently. Pick an incident response team and assign a leader. Make sure the team includes a member of executive management. Define roles and responsibilities so that everyone is clear as to

who is responsible for what should an incident arise. Communicate to everyone at your company who to contact if they suspect a Cyberincident has occurred (or is occurring). Gather and distribute after-hours contact information for your incident response team. Next, outline the basic steps of your incident response plan by establishing checklists and clear action items.

Introduction

California's 3.5 million small businesses are crucial to the State's economic vitality. They represent 99.2 percent of all employers, and employ more than half of all workers in the private sector. Small businesses are crucial to the fiscal condition of the state.[4] Key facts about small businesses in California include:

- Small businesses in California employ more than 8.7 million workers.[5]
- 80.3% of small businesses in California do not have employees.[6]
- Most small businesses (90.0%) have fewer than 20 employees.[7]
- Small businesses account for 50% of gross domestic product and more than 60 percent of new jobs.[8]

Today, small businesses depend upon technology for all aspects of their operations. Specifically, online applications, social media, and Internet-connected mobile devices and applications are key tools for many critical business functions. Notable trends include:

- 98% of small businesses report that they use wireless technology, up from 88% in 2007.[9]
- 85% of small businesses reported using smartphones for their operations, more than double the usage in 2007.[10]
- 67% of small businesses are using their website to market to customers.[11]
- 41% of small businesses use email to market to customers.[12]
- 41% of small businesses report that all their employees use wireless devices or wireless technologies to work away from the office.[13]
- The use of social media by small businesses continues to increase with 41% using Facebook and 36% using LinkedIn.[14]
- Nearly one-third of small businesses use mobile-friendly websites to engage with customers.[15]

- 31% of small businesses use mobile apps. Of small businesses using mobile apps, GPS navigation and mapping are used by 74%, followed by location-based services (43%); document management (35%); social media marketing (32%); and mobile payments in the field (30%).[16]

In just the first three months of 2013, there were more than one billion Cyberattacks.[17] This makes clear that the threat is very real and the statistics show that the number of small businesses that are victims of cybercrimes is growing rapidly. This victimization occurs either through scams, fraud, theft, or other malicious criminal activity.

Customers and employees expect that businesses will provide adequate and appropriate protection for their personal information. Additionally, current and potential business partners want assurance that their information, systems, and networks will not be put at risk when they do business with you. They rightly expect an appropriate level of security from their business partners. Responsible small business owners must protect sensitive information. In fact, with some kinds of information, business owners must abide by special, much more restrictive, statutorily mandated security requirements. For example, failing to properly protect health information can result in significant fines and penalties.

In 2012, 50 percent of all targeted attacks were aimed at businesses with fewer than 2,500 employees. More significantly, businesses with fewer than 250 employees were the target of 31 percent of all cyberattacks.[18] This is especially bad news, because based on research conducted by the National Cybersecurity Alliance, many small businesses believe they are immune to cyberattacks.[19] While some small business owners may assume that they have nothing of value to a cybercriminal, they forget that they retain customer information, create intellectual property, and keep money in the bank. Espionage, though mostly thought to be targeted at governments and defense contractors, is often directed at businesses so small they do not even have IT personnel.[20] Small businesses may also have access to their business partner's computer systems as part of an integrated supply chain or sensitive data and intellectual property. Though it can be argued that the rewards of attacking a small business are less than what can be gained from a large enterprise, this is offset by the fact that most small businesses dedicate fewer resources to protecting their information assets and are therefore easy targets.

Given that small businesses are potential targets for cybercrime, small business owners should take prudent steps to manage this risk and establish a plan in the event of a cyberattack. While more than two-thirds of small businesses claim the Internet is critical to their business success, only 10 percent have formal Internet security policies[21] and just 29 percent provide any training to employees on Internet safety and security.[22] Failing to take these steps puts small businesses at risk of incurring financial losses and data breaches, which may also come with financial costs depending on the type of data lost in the breach.

The High Cost of Cybercrime

According to the 2013 Cost of Cybercrime Study, conducted by the Ponemon Institute, the average cost to victims of a data breach per compromised record is now $136, or $157 if it results from malicious criminal conduct.[23] Additionally, the Study notes that costs for businesses that are victims of Internet-based attacks have risen 78 percent per year, on average, over the past four years.[24] And from 2010 through 2013, the time needed to recover from a breach has increased 130 percent.[25] Just as there is a cost involved in cybersecurity protection, there is a cost involved in not protecting the information stored in your systems. These case examples are proof of the high cost of cybercrime:

- Bank of the West – A 2012 Christmas Eve Cyberattack against the Web site of a regional California financial institution helped to distract bank officials from an online account takeover against one of its clients, netting cyberthieves more than $900,000.[26]

- Efficient Services Escrow Group – In 2013, cybercriminals stole $1.5 million in a cyberheist against a California escrow firm. The company was forced to close and lay off its entire staff. Meanwhile, the firm's remaining money is in the hands of a court-appointed state receiver who is preparing for a lawsuit against the victim's bank to recover the stolen funds. The bank's systems were compromised by a remote access Trojan prior to the heist.[27]

- Target – Between Nov. 27 and mid-December 2013, Target fell victim to a massive data breach. Their estimates state that the email, mailing address, phone numbers, and financial information of between 70 million to 110 million customers was stolen. Just after the hack there was a ten-to-twentyfold increase in the number of high-value stolen

cards on black market websites. After the breach, customers became wary of shopping. While Target began the fourth quarter with self-reported "stronger than expected" sales, following the breach announcement, sales were "meaningfully weaker than expected." Target is now expecting a comparable sales decline of 2 to 6 percent for the remainder of the quarter.[28]

- Neiman Marcus – Neiman Marcus has confirmed that it learned of a large-scale data breach on January 1, 2014. It currently appears the breach was active from mid-July 2013 through the end of October 2013 and involves payment card information. Neiman Marcus has disclosed that over one million payment card accounts were possibly impacted by the breach, but has said that debit card PINs and customer social security numbers and birthdates were not compromised.

- Michaels Stores – Michaels recently announced that it had been notified of possible fraudulent activity on some U.S. payment cards that had been used at Michaels, but has not yet confirmed any specific customer data was accessed. Michaels has said that if their investigation reveals that any customers were affected, that they will offer identity protection and credit monitoring services at no cost.

California law requires organizations with customers and/or employees in the state of California to disclosure security breaches where there is a reasonable belief that unauthorized access to unencrypted personal information has occurred. A breach is defined as unauthorized access to, or acquisition of, electronic data that potentially compromises the security, confidentiality, or integrity of personal information. The average estimated cost for these notifications and associated security breach costs is well over $130 per victim whose information was released in the breach.[29]

The recommendations offered in this Guide are not regulations, mandates or legal opinions. Rather, they provide an overview of the cybersecurity threats facing small businesses, a brief and incomplete summary of several best practices that help manage the risks posed by these threats, and a response plan in the event of a cyberincident. Small businesses seeking additional information are encouraged to review the forthcoming National Institute of Standards and Technology Cybersecurity Framework[30], to be released in February 2014, which will offer guidance and resources to businesses on how to more effectively manage cybersecurity risk. Businesses with credit card payment information should also consult to PCI Data Security Standards. See *https://www.pcisecuritystandards.org/security_standards/*

Cybersecurity Threats Facing Small Businesses

Advances in online technology have made many of the day-to-day tasks of running a small business substantially easier. Even traditional brick and mortar stores have come to benefit from these advances through services like low cost, Internet enabled point of sale (POS) systems or cloud-based payroll and inventory services that process and store sensitive data that previously resided on local hard drives or in filing cabinets.

These technological advances offer many advantages, but have also introduced a number of new security risks. An increasing amount of sensitive business data is now digitized and stored on computers, tablets, smartphones, and a range of third-party servers via online services. Data is more accessible and replicable than ever before and this, in turn, has made it more vulnerable to unauthorized access and distribution.

Fortunately, general awareness and some relatively simple security precautions can protect companies against the majority of the security threats they will face today. Security threats can be broadly categorized into the following categories:

1. Social Engineering Scams
2. Network Breaches
3. Physical Breaches
4. Mobile Breaches

This Guide describes each of these categories and details the different types of threats that comprise them.

Social Engineering Scams

Social engineering is a common technique that bad actors use in order to gain access to your device, network, or information. The motivation of these types of scams is most often greed. These scams can be either technologically sophisticated (an email that seems to come from a trusted vendor that actually contains malware) also known as Phishing or incredibly low tech (like the Nigerian e-mail or "419" scams).

Small businesses may find themselves the victims of phishing attacks by criminals seeking access to their customer database or bank accounts. In 2012, one in 291 emails contained a virus or link to malware.[31] According to Verizon, 29% of unauthorized accesses in 2012 involved some form of social engineering.[32]

Phishing attacks have become more sophisticated in recent years as the online footprints of individuals have grown. Social networks have given phishers access to a treasure trove of personal information they can use to customize their attacks and increase their likelihood of success. It sometimes only takes one employee to fall for a targeted attack and compromise their sensitive corporate credentials for an entire company to suffer.

Network Breaches

Malware

Malware, which is short for "malicious software," is any type of program designed or used for unauthorized access to a computer system. According to the cybersecurity company FireEye, malware continues to be the cyberweapon of choice. Malware activity has become so pervasive that once every three minutes, an organization will experience a malicious email file attachment or web link as well as malware communication—or call-back—to a command and control (CnC) server.[33]

Malware can be used to access data, control a targeted system, or to do both. Malware used to access data ranges from simple programs that track keystrokes and copy screenshots to sophisticated programs that can search through a users files and browser history to steal passwords and bank data. Malware used to control a target system, or control style malware, disrupts or locks a user's system. Control style malware can also be used to take over a legitimate website's servers, endangering that site's visitors by making them accessible to further attacks that exploit their browser's vulnerabilities.[34] The most advanced types of malware allow attackers to both access and control the victim's system. The attacker can first access the data stored on the target device and then use that device to access other computers, tablets, and cell phones in the target's network.[35] An entire organization can be compromised from a single unsecured device. While malware has historically targeted only computers, 'mobile malware' that targets tablets and smartphones is an increasing threat.[36] Terms often used in security news stories like viruses,

worms, Trojans and spyware describe specific types of malware, which are explained in the classification table below:

Malware Types

Virus	A form of malware that relies on human interactions (such as downloading or opening files) to spread.
Trojan	A form of malware that masquerades as a legitimate application.
Worm	A form of malware that can self-replicate and distribute itself across multiple devices without human intervention.
Spyware	A form of malware that discreetly captures and transmits sensitive information from a device (like keystrokes or webcam photos).
Adware	A form of malware whose primary purpose is to serve obtrusive or unexpected ads on the compromised device.
Chargeware	A form of malware that charges the victim money without his/her knowledge or consent.
Ransomware	A form of malware that restricts access to a device unless the victim pays to have it unlocked.

Devices in the workplace can become infected by malware through a number of different means, such as opening a malicious email attachment, visiting an infected website, downloading a mobile application, or clicking on an unknown link on social media platforms such as Twitter. The damage that comes from a malware infection ranges from the relatively benign such as intrusive popup ads on a desktop computer, to the downright dangerous. For example, if a business' website is compromised by malware, then search engines like Google may flag the site as a security risk to potential customers, which can negatively impact sales and revenue.

The risk of malware infection depends largely on the behavior of device users. Engaging in risky behaviors, such as downloading applications outside of traditional app stores,

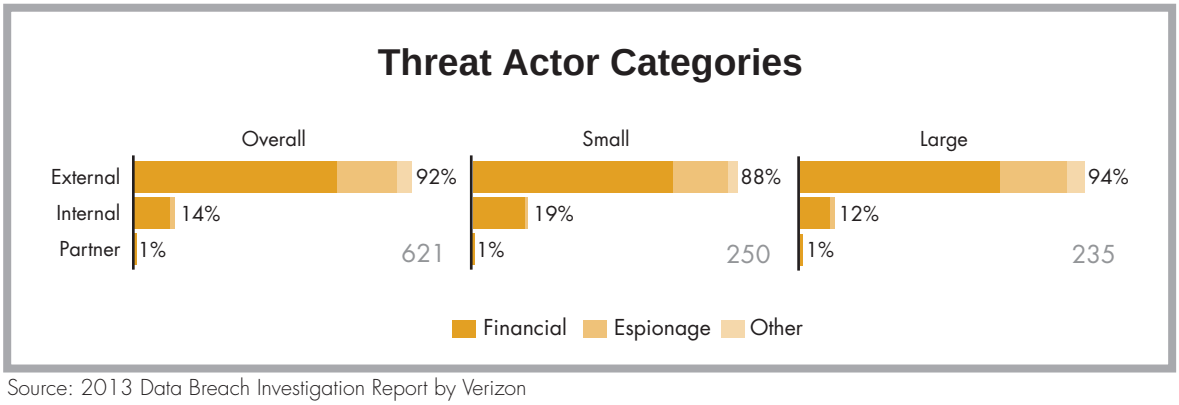
visiting sites promising to download or stream pirated materials, or clicking links in suspicious emails, will raise the probability of encountering malware. When it comes to mobile malware, Lookout, an internet security company, documented a significant increase in malware detections last year, with toll fraud malware (malware that bills unsuspecting victims through premium SMS services) emerging as the most significant threat.[37] In 2013, a Lookout investigation found evidence that the development of malware for mobile devices has transitioned from an individual venture to a veritable industry in which complexly organized groups that resemble corporations both develop and distribute mobile malware for profit.[38]

Unsecured Internet Connections

Many employees work from home, hotels, airports, and coffee shops. This means they are likely using a variety of wireless internet connections to respond to email and access sensitive corporate accounts and data. Businesses do not have direct control over these wireless access points like they do in the workplace, and these unsecured connections risk exposing company data when security measures are not taken to protect the transmission of data.

Weak Passwords and Encryptions

In many instances, passwords are the only things protecting our financial data, trade secrets, and identifying information. Businesses must be vigilant in ensuring they use a variety of complex passwords that change often. Hackers can use special software to "guess" passwords or they can trick unsuspecting employees into turning over their login credentials by directing them to seemingly legitimate login pages. Breaches are more common than we'd like to think and many go unreported or undiscovered. According to Verizon's 2013 Data Breach Investigation Report[39], most breaches are perpetrated by hackers:



Source: 2013 Data Breach Investigation Report by Verizon

In 2012, the California Attorney General's Office received 131 reports of data breaches by businesses, affecting the personal information of more than 2.5 million Californians.[40] That said, there is also the risk that a current, or former, employee executes a data breach.

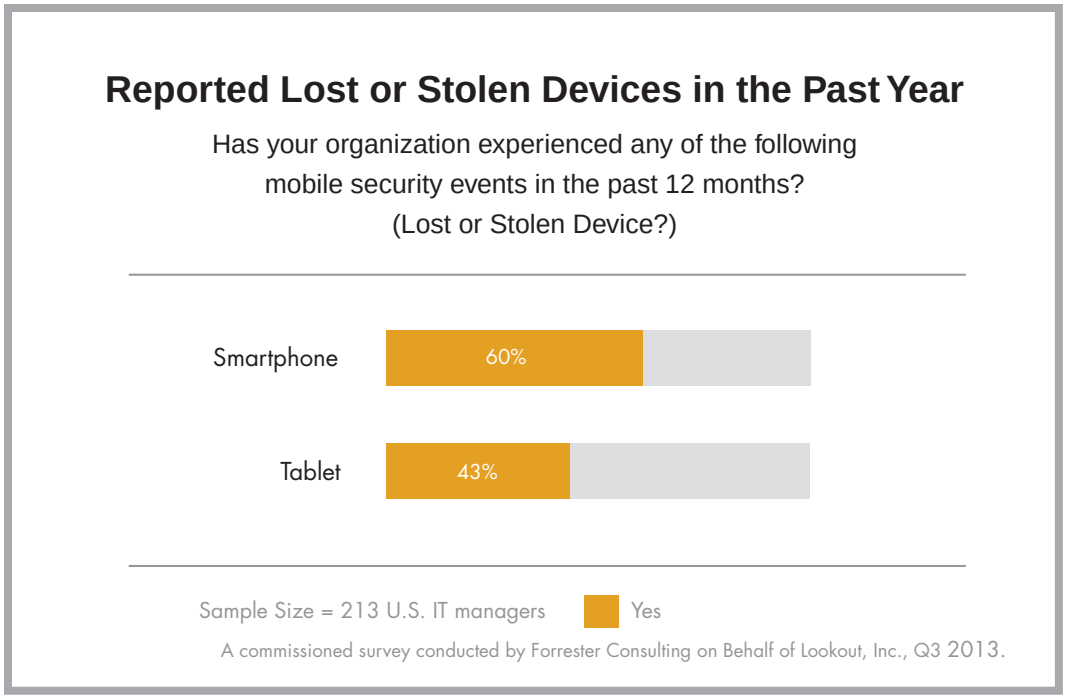
Physical Breaches

Device Theft & Loss

The amount of data that can be stored on laptops, tablets, and smartphones is truly incredible. For many small businesses, a single smartphone may store multiple years worth of the company's financial and inventory records. Moreover, what sensitive data isn't stored on these devices directly is often accessible via online storage services that allow users to remotely access gigabytes worth of company data in the cloud.

As laptops, smartphones, and tablets have become ubiquitous in the workplace, the risk of theft or loss of workplace devices has risen. Employees use their devices at home or on the road to conduct work and if they accidentally leave them in a cab, or suffer a break-in, these devices and the corporate data on them could end up in the wrong hands. In San Francisco, for example, nearly half of all robberies in 2012 involved smartphones[41], and it is highly likely that a number of those robberies involved phones with access to sensitive business data.

A Lookout survey of business IT admins in the Fall of 2013 found that dealing with the theft or loss of employee devices was a common experience:



Source: 2013 Data Breach Investigation Report by Verizon

Foreign Contact

Many small businesses in California have relationships with foreign partners that require their employees to travel abroad to maintain or manage business operations. Business should be aware that foreign travel might incur additional security risks, as some countries have more aggressive search and seizure policies when it comes to electronic devices and the data contained on them. Internet communications may be closely monitored and recorded in some foreign countries, so companies should be aware that their businesses communications in another country may subject to foreign corporate espionage and/or government surveillance. There have been reports, for example, of American business travelers in China having their laptops compromised with spyware, despite having left those laptops in locked hotel rooms.

Mobile Breaches

Given the presence of mobile devices such as phones and tablets, business owners are encouraged to focus on the unique nature of mobile threats. Like viruses and spyware that can infect a PC, there are a variety of security threats that can affect mobile devices in the workplace. In addition, some employers allow their employees to use their own personal devices to conduct business. This can means anything from an employee adding company email to their personal smartphone to requiring employees to bring their own laptops to work on in the office. This workplace trend – known as Bring Your Own Device (BYOD) – raises unique security challenges as employers must balance the need to protect corporate data and systems with employees' desire for convenience and privacy on their personal devices.

Device theft and loss aside, mobile threats fall into several categories: application-based threats, web-based threats, and network-based threats:

- Application-Based Threats
  Unfortunately, not all mobile apps can be trusted. So called "malicious apps" may look fine on the surface, but they are specifically designed to commit fraud or cause disruption to devices. Even perfectly legitimate apps can pose a threat if exploited for fraudulent purposes. Application-based threats may come in the form of malware (discussed earlier in this report), but also include:

1. **Privacy threats –** These apps may not be malicious in design; they gather or use sensitive information (e.g., location, contact lists, personally identifiable information) beyond what is necessary to perform their function, and

2. **Vulnerable apps –** These are apps that contain flaws that can be exploited for malicious purposes. Vulnerabilities in these apps may enable an attacker to access sensitive information, perform undesirable actions, or download other apps to your device without your knowledge.

- Web-Based Threats

  Mobile devices are constantly connected to the Internet and can access web-based services, exposing mobile devices to additional threats like:

  - Phishing Scams that may use email, text messages, Facebook or Twitter to distribute links to malicious webpages designed to trick you into providing information like passwords or account numbers. Often these messages and sites are very different to distinguish from those of your bank or other legitimate sources.
  - Drive-By Downloads can automatically download an application when you visit a web page. In some cases, you must take action to open the downloaded application, while in other cases the application can start automatically.
  - Browser exploits take advantage of vulnerabilities in your mobile web browser or software launched by the browser such as a Flash player, PDF reader, or image viewer. Simply by visiting an unsafe web page, you can trigger a browser exploit that can install malware or perform other actions on your device.

- Network Threats

  Mobile devices typically support cellular net works as well as local wireless networks (like WiFi or Bluetooth). Both types of net works can host different classes of threats:

  - Network exploits take advantage of flaws in the mobile operating system or other software that operates on local or cellular networks. Once connected, they can install malware on your phone without your knowledge.

- Wi-Fi Sniffing intercepts data as it is traveling through the air between the device and the WiFi access point. Many applications and web pages do not use proper security measures, sending unencrypted data across the network that can be easily read by someone who is grabbing data as it travels.

Practical Steps to Minimize Cyber Vulnerabilities

Assume You're a Target

Small size and relative anonymity no longer ensure that you will be left alone. Targeted attacks threaten small companies as well as large ones. Just as it has become second nature for most of us to lock our front doors when we leave the house, assume you are a potential target and take basic precautions to protect yourself from cybercrime. Also, make sure your business organization has a plan for how to respond to a cyberincident.

Lead by Example

Cybersecurity is not simply the province of the IT person; it requires the leadership and dedication of small business owners. Small business owners are uniquely positioned to ensure that they and their employees are following good cybersecurity practices. They are also in the best position to understand their company's network and the devices that connect to it. This requires dedicating the time and resources necessary to ensure the safety and security of information assets.

Bank Securely

It is essential that small business owners put security first when they engage in online banking. This means that it should only be done using a secure browser connection (indicated by "https" and/or a lock visible in the address bar or in the lower right corner of your web browser window). Online banking sessions should be conducted in the private mode of your web browser and you should erase your web browser cache, temporary Internet files, cookies, and history afterwards so that if your system is compromised, that information will not remain on your system to be stolen by cybercriminals. In addition, take advantage of the security options offered by your financial institution. Examples include using two-factor authentication to access your account, requiring that two authorized individuals sign off on every transfer of funds, and setting up account notifications by email or text message when certain activities occur on your account.

- Account notifications – Most banks offer customers the ability to set up text or email notifications to alert them to certain activities on their account.

- Two-factor authentication – Try to get a bank account that offers some form of two-factor authentication for online banking. Two-factor authentication adds an auto-generated passcode that is only valid for a short period of time and is required in addition to your login credentials in order to gain access to your online account.

- Segregate Responsibilities – Do not allow a single individual to both initiate and approve financial transactions. The unfortunate truth is that insiders – those who work in a business – are the source of most security incidents in the business. When they perform harmful actions (deliberately or otherwise), your business suffers.

Defend Yourself

Emphasize multiple, overlapping, and mutually supportive solutions to guard against single-point failures in any specific technology or protection method. This should include the deployment of regularly updated firewalls, antivirus, and web security solutions throughout the network. Also, anything connected to your network should be secured by more than signature-based antivirus technology.

- Firewalls – Install, use, and keep updated a software firewall on each computer system used in your small business. While most operating systems include some type of firewall, there are commercially available software firewalls that are reasonably priced or free. Since your employees may do some work at home, ensure that they install and keep operational firewalls on their home systems. It is necessary to have software firewalls on each computer even if you have a hardware firewall protecting your network. This is necessary in the event your hardware firewall is compromised by a hacker or by malicious code of some kind.

- Anti-Virus Software – Install, use (in "real-time" mode, if available), and keep regularly updated anti-virus and anti-phishing software on every device used in your business, be it a laptop, tablet or smartphone. Anti-virus software with anti-spyware capabilities is available at a reasonable price from multiple vendors. Vendors now offer subscriptions to "security service" applications, which provide multiple layers of protection of security protection (in addition to anti-virus and anti-spyware protection). Given that your employees may do work at home, it is a good idea to obtain copies of your business anti-virus software for employees' home computers.

- Secure connectivity – Most businesses have broadband (high speed) access to the Internet. It is important to keep in mind that this type of Internet access is always "on." Therefore, your computer - or any network your computer is attached to - is exposed to threats from the Internet on a 24 hour a day/7 day a week basis. For broadband

Internet access, it is critical to install and keep operational a hardware firewall between your internal network and the Internet. This may be a function of a wireless access point/router or may be a function of the router provided by your Internet Service Provider. For these devices, change the administrative password upon installation and regularly thereafter. It is a good idea to change the administrator's name as well.

Educate Employees

Nobody enjoys "mandatory" training, but educating your employees on how to avoid, detect and effectively report cyberincidents is essential to reducing the risk associated with a cyberincident. The threats we face in this area are evolving; this means that practices that might have kept your data reasonably secure in 2010 might not be adequate in 2013. More importantly, keep in mind that cybersecurity is a "weakest link" type of risk management issue. This means that you can invest all you want in expensive security technology, but if your employees aren't safety conscious, those measures will be easily defeated. Educate your employees as to why it's important to never click on a hyperlink, or open a file, from an unknown or untrusted source. Employees need to understand that even if they do not have access to data they would consider valuable, they can still be targeted as an avenue to access another computer that does have valuable data. Every employee must take information security seriously. After this training, they should be requested to sign a statement that they understand these business policies, that they will follow those policies, and that they understand the penalties for not following those policies. Having your employees trained in the fundamentals of cybersecurity is one of the most effective investments you can make to better secure your business information, systems, and networks. You want to develop a "culture of security" in your employees and in your business.

Protect Your Data

To effectively protect your data, you first need to know the types of data you have and where it is. As businesses change and grow, data is often moved or archived to multiple locations, both on and off site. These stockpiles of potentially sensitive data can be lost or forgotten, especially if the staff responsible for managing this data has turned over. Small businesses should comprehensively review what data they have stored on their IT systems, both on site and off, and with third parties (include backup tapes and cloud computing

solutions in your data mapping project). Once you've comprehensively mapped the data, take a hard look and get rid of what you don't really need.

- Encryption – It is important to encrypt the data you have on your systems. Encryption essentially scrambles data so that it is unreadable by anyone without a special key. Free and easy to use encryption technology is widely available. Encrypting your data can dramatically reduce your exposure to a data breach and the theft of proprietary information. Moreover, by encrypting your data you may effectively avert the need to disclose a data breach to your customers and third parties because California's state disclosure laws specifically exempt encrypted data. Applications such as Symantec PGP, TrueCrypt, Microsoft's BitLocker and Apple's FileVault 2 provide full disk encryption for both laptops and desktops that can be used to protect your data. It is also important to use strong encryption so that data being transmitted between your computers and the wireless access point cannot be easily intercepted and read by electronic eavesdroppers. The current recommended encryption is Wi-Fi Protected Access 2 (WPA-2) – using the Advanced Encryption Standard (AES) for secure encryption.

- Limit Access – Do not provide any one employee access to all data. Do not provide any one employee access to all systems (financial, personnel, inventory, manufacturing, etc.). For all employees, provide access only to those systems and the specific information that are necessary to do their jobs. Machines that handle sensitive information like payroll or point of sale (POS) functions should be separate from machines that do routine services, like updating Facebook and checking email. Also, make sure you disable and purge old user accounts; experience has shown these can become vulnerabilities. User accounts should be disabled at the time of an employee's departure.

- Back up Important Data – Back up important data on each computer used in your business. It is necessary to back up this data because computers die, hard disks fail, employees make mistakes, and malicious programs can destroy data on your computers. Without data backups, you can easily get into a situation where your data is lost completely or you have to recreate your data from paper copies and other manual files. You should back up data on a monthly basis and test your backups to ensure they can be read.

- Securely Dispose of Stored Data – When disposing of old computers, remove the hard disks and destroy them. You can destroy a hard disk by beating the hard disk platters with a hammer or you can use a drill with a long drill bit and drill several holes through the hard disk. In addition, when disposing of old media destroy any containing sensitive business or personal data.

Be Password Wise

Change any default username or passwords for computers, printers, routers, smartphones, or other devices. ANYTHING is better than the default. Specifically, you should use strong passwords and don't let your Internet browser remember your passwords.

- Strong Passwords – As simple as it sounds, requiring strong passwords can dramatically reduce your vulnerability to a cyberincident. The strength of a password is determined primarily by its length (at least 8 characters long) and complexity (good passwords consist of a random sequence of letters, numbers, and special characters). It is important to change your passwords frequently (every three months is a good rule of thumb). And avoid using personal information such as your birthday, college, or kids' names. As tempting as it may be, don't use the same passwords for personal and work use, and don't write all your passwords down in one place.

- Unique Accounts – Each of your employees should have an individual account with a unique username and password. Without individual accounts for each user, you may find it difficult to hold anyone accountable for data loss or unauthorized data manipulation.

Operate Securely

Keep your operating system secure by keeping all operating systems and software up to date. Don't install any software you did not specifically seek out, keep your software up to date, and remove or uninstall software you are no longer using.

- Update Software – All operating system vendors provide patches and updates to their products to correct security problems and to improve functionality. Microsoft provides

monthly patches on the second Tuesday of each month. From time to time, Microsoft will issue an "off schedule" patch to respond to a particularly serious threat. When you purchase a new computer, be sure to update the operating system immediately. Office productivity products such as Microsoft Office also need to be patched & updated on a regular basis. For Microsoft products, the patch/update process is similar to that of the Microsoft Windows operating systems. Other business software products like Adobe Reader also need to be updated regularly.

- Avoid software from any unknown sources – Only download software from those organizations with which you have a trusted business relationship.

- Limit Administrator Privileges – To better protect systems and information, ensure that computer accounts used by employees do not have administrative privileges. This will stop most attempts – automated or not – to install unauthorized software. If an employee uses a computer with an administrative user account, then any malicious code that they activate (deliberately or by deception) will be able to install itself on their computer.

- Social Media – Enforce a social media policy to prevent employees from posting corporate information on Facebook, Twitter, LinkedIn, etc. Only the marketing department should be allowed to post any information and they should closely review anything to be posted to ensure it is not sensitive and that it does not reveal information an attacker would find useful in social engineering or other attacks.

- Background Checks – Perform background checks on key employees (all executives, all finance personnel, and anyone with administrator access (e.g. IT staff)).

- Ensure corporate wireless networks are properly secured. Use WPA2 Enterprise.

- Do not use public (i.e. non-corporate) wireless connections to conduct any company business, such as checking email, unless you are using a secure connection (e.g. corporate VPN access and/or an SSL protected web email server).

Basic Guidance on How to Respond to CyberIncidents

As vital as it is to focus on the prevention of cybercrime, it is also important to recognize that no preventative measures are completely effective. Cybersecurity experts commonly recommend that business executives adopt a "not if but when" mentality – that is, assume that at some point in the foreseeable future, your company will have to cope with a cyberincident of some type, and plan accordingly. To that end, every small business should put together a "game plan" so that when a Cyberincident happens, your resources are used wisely and efficiently. Experience has shown that many organizations wait until they have actually suffered a serious data breach before attempting to come up with a process for dealing with such a situation – which amounts, effectively, to building an airplane in the air.

An effective incident response ("IR") plan will likely lead to faster and better choices, which in turn will help to mitigate any damage that may have been caused.

Form Your Incident Response Team

Depending on the size of your business, it may not be immediately clear who should be responsible for responding to a Cyberincident. As a result, it is critical to pick an incident team and assign a team leader. Don't instinctively delegate IR responsibilities entirely to "IT staff" – indeed, we recommend that your IR team include a member of your executive team and in-house counsel if you have one. This is because even seemingly minor incidents (like a lost laptop) can give rise to complex, fast-moving and potentially costly decisions that can seriously impact your business.

In forming your IR team, define roles and responsibilities so that everyone is clear as to who is responsible for what should an incident arise. Communicate to everyone at your company who to contact if they suspect a Cyberincident has occurred (or is occurring). Gather after-hours contact information for your IR team members and distribute this information to all staff. Also, think through channels of communications that do NOT involve work-provided phones and email, as these may be compromised during a serious Cyberincident.

Response Planning

Next, outline the basic steps of your IR plan by establishing checklists and clear action items. For example, your incident response plans might include the following basic steps to address a serious data breach or malware incident:

a. Don't turn off your computer. Turning off your computer might seem like the instinctual first step but often will destroy evidence and erase valuable clues that will allow a forensic expert to fully assess the attack.

b. Contact law enforcement. Many local law enforcement offices have computer or e-crime sections that are experienced in investigating and helping with these types of attacks.

c. Document the potential scope of the breach. Establish current facts about the breach and communicate them as appropriate. These facts may include why administrators suspect a breach, the number of systems accessed and the data that may have been stolen. Executives should be kept apprised of the facts as they evolve, measures taken to date, measures that will be taken and what to expect going forward.

d. Determine notification requirements. Identifying, assessing, containing, remediating and reporting a breach is challenging. You will need to determine if outside help is required. Questions to consider include whether you have the capabilities to respond to the incident internally and whether you need to engage a forensic investigator and/or expert legal counsel.

e. Determine if outside help is required and, if necessary, contact an IT security professional. Identifying, assessing, containing, remediating and reporting a breach is challenging. You will need to determine if outside help is required. Questions to consider include whether you have the capabilities to respond to the incident internally and whether you need to engage a forensic investigator and/or expert legal counsel.

f. Determine notification requirements. Retain system, application, database and network device logs and avoid making changes to the system suspected of being compromised before data is preserved. You may wish to consult an expert to assist you in acquiring a forensic image of the hard drives and live memory of the systems suspected of being compromised and following proper chain of custody procedures.

We recommend that your organization come up with, and document, specific policies and procedures that will be implemented in specific situations. In other words, come up with a plan for each type of incident that your company might experience: a lost computer, smart phone or thumb drive containing unencrypted data, an external data breach or theft of intellectual property, malware, or cyber extortion. For each of these scenarios, create and

write up an easily accessible quick-response guide. The FCC provides a guide to creation of a cybersecurity plan. The information may be found here: *http://www.fcc.gov/cyberplanner*

As you create your IR team and plan, it would be wise to form relationships with key third parties, such as local law enforcement. Also, it makes sense to get to know a few cybersecurity experts so that you have their contact information handy just in case.

Your IR plan should address procedures necessary to adequately document the details of a particular incident (including a timeline of events, preservation of compromised systems if necessary, as well as who was involved and what your response was). If the incident involved the possible disclosure of unencrypted personally-identifiable information (PII) or payment-card-information (PCI), consult with a lawyer to ensure you comply with all legal disclosure requirements. For example, California law requires a business or state agency to notify any California resident whose unencrypted PII or PCI, as defined, was acquired, or reasonably believed to have been acquired, by an unauthorized person.[42] Finally, your IR plan should have a process to review your preventative cybersecurity measures and your IR response plan after every Cyberincident.

End Notes

[1] Kamala D. Harris, 2012 Attorney General Breach Report, (July 1, 2013) <*http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-releases-report-data-breaches-25-million*> (as of Jan. 8, 2014).

[2] 75% of attacks are considered "opportunistic". Verizon RISK Team, Verizon Data Breach Investigations Report, p. 6 <*http://www.verizonenterprise.com/DBIR/2013/*> (as of Jan. 9, 2014)

[3] Symantec, Internet Security Threat Report 2013: Volume 18 (April 2013) p. 4. <*http://www.symantec.com /security_response/publications/threatreport.jsp*> (as of Jan. 7, 2014)

[4] Office of Advocacy, The U.S. Small Business Administration, 2012 Small Business Profile for California, (February 2013) < *http://www.sba.gov/advocacy/848/468011*> (as of Jan. 9, 2014).

[5] Calculated using Labor Market Data from EDD (Seasonally adjusted average for 2013) and small businesses comprising 52% of Employment, Governor's Office of Business and Economic Development, *California by the Numbers* (October 2013) at 2.

[6] Ibid.

[7] Ibid.

[8] Ibid.

[9] 2013 AT&T Small Business Technology Poll, AT&T Inc. <*http://www.att.com/gen/press-room?pid=23878*> (as of Jan. 9, 2014).

[10] Ibid.

[11] Ibid.

[12] Ibid.

[13] Ibid.

[14] Ibid.

[15] Ibid.

[16] Ibid.

[17] SBA Office of Advocacy, "Advocacy Points out Small Business Concerns Regarding the Preliminary Cybersecurity Framework", <*http://www.sba.gov/sites/default/files/Cybersecurity%20Fact%20Sheet_0.pdf* > (as of Jan. 9, 2014)

[18] Symantec, Internet Security Threat Report 2013: Volume 18 (April 2013) p. 4. <*http://www.symantec.com/security_response/publications/threatreport.jsp*> (as of Jan. 7, 2014).

[19] National Cyber Security Alliance, Symantec, 2012 NCSA/ Symantec National Small Business Study p. 9 < *http://www.staysafeonline.org/stay-safe-online/resources/*> (as of Jan. 9, 2014)

[20] Verizon RISK Team, Verizon Data Breach Investigations Report, p. 15-16 <*http://www.verizonenterprise.com/DBIR/2013/*> (as of Jan. 9, 2014)

[21] National Cyber Security Alliance, Symantec, 2012 NCSA/ Symantec National Small Business Study (fact sheet), p. 1-2 <*http://www.staysafeonline.org/stay-safe-online/resources/*> (as of Jan. 7, 2014)

[22] National Cyber Security Alliance & Symantec, 2012 National Small Business Study, p. 6 <*http://www.staysafeonline.org/stay-safe-online/resources/*> (as of Jan. 9, 2014)

[23] Ponemon Institute, 2013 Cost of Data Breach Study: Global Analysis, p. 8 <*http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=ponemon-2013*> (as of Jan. 16, 2014)

[24] Willie Jones, "How Much Does Cybercrime Cost? $113 Billion", (Nov. 22, 2013) *http://spectrum.ieee.org/riskfactor/telecom/security/how-much-does-cybercrime-cost* (as of Jan 16, 2014)

[25] Ibid.

[26] Brian Krebs, "DDoS Attack on Bank Hid $900,000 Cyberheist", (Feb. 19, 2013), Krebs on Security <*http://krebsonsecurity.com/2013/02/ddos-attack-on-bank-hid-900000-cyberheist/*> (as of Jan. 7, 2014)

[27] Brian Krebs, "$1.5 million Cyberheist Ruins Escrow Firm", (Aug. 7, 2013), Krebs on Security <*https://krebsonsecurity.com/2013/08/1-5-million-cyberheist-ruins-escrow-firm/*> (as of Jan. 7, 2014)

[28] Elizabeth Harris and Nicole Perlroth, "For Target, the Breach Numbers Grow", (Jan. 10, 2014), New York Times *http://www.nytimes.com/2014/01/11/business/target-breach-affected-70-million-customers.html?_r=0* (as of Jan. 10, 2014)

[29] Ponemon Institute, 2013 Cost of Data Breach Study: Global Analysis, p. 1 <*http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=ponemon-2013*> (as of Jan. 9, 2014)

[30] The National Institute of Standards and Technology, Executive Order 13636: Cyber security Framework, (Nov. 12, 2013) <*http://www.nist.gov/cyberframework/*> (as of Jan. 16, 2014)

[31] Symantec Corporation, Internet Security Threat Report 2013 :: Volume 18 (April 2013) p. 46. <*http://www.symantec.com/security_response/publications/threatreport.jsp*> (as of Jan. 7, 2014).

[32] Verizon RISK Team, 2013 Data Breach Investigations Report, p. 36 *http://www.verizonenterprise.com/DBIR/2013/* (as of Jan. 7, 2014)

[33] FireEye, Inc., FireEye Advanced Threat Report (April 2013) <*http://www.fireeye.com/blog/technical/malware-research/2013/04/the-new-fireeye-advanced-threat-report.html*> (as of Jan. 16, 2014)

[34] Symantec Corporation, Internet Security Threat Report 2013 :: Volume 18 (April 2013) p. 26-27. <*http://www.symantec.com/security_response/publications/threatreport.jsp*> (as of Jan. 7, 2014).

[35] Symantec Internet Security Threat Report 2013, supra.

[36] Id. at 37.

[37] Lookout, Inc., State of Mobile Security 2012 <*https://www.lookout.com/resources/reports/state-of-mobile-security-2012*> (as of Jan. 8, 2014)

[38] Lookout, Inc., Dragon Lady: An Investigation Into the Industry Behind the Majority of Russian-Made Malware <*https://www.lookout.com/resources/reports/dragon-lady*> (as of Jan. 8, 2014)

[39] Verison RISK Team, Verison Data Breach Investigations Report <*http://www.verizonenterprise.com/DBIR/2013/*> (as of Jan. 9, 2014)

[40] Kamala D. Harris, 2012 Attorney General Breach Report, (July 1, 2013) <*http://oag.ca.gov/ news/press-releases/attorney-general-kamala-d-harris-releases-report-data-breaches-25-million*> (as of Jan. 8, 2014).

[41] Terry Collins, "Stolen iPhones And Other Smartphones Have Become A Nationwide Problem", (Oct. 20, 2012), The Huffington Post <*http://www.huffingtonpost.com/2012/10/20/stoleniphones_n_1992843.html*> (as of Jan. 8, 2014)

[42] Cal. Civil Code Sections 1798.29(a) and 1798.82(a).