CYBER-SECURITY FOR THE SMALL AND MEDIUM SIZE BUSINESS

INTRODUCTION

Small and medium size businesses ("SMBs") are often targeted by cyber criminals as they are perceived as the weakest link. SMBs with sensitive and confidential data must protect it from the same threats as larger companies but with vastly different resources. As a result, SMBs must marshal the resources available to them to harness practical solutions which will sustain an environment secure from the deluge of cyber threats present in the digital world. This process will fundamentally involve understanding the threats and the resulting risks to your company from a cyber-attack, and implementing effective controls to protect your business. If you ignore your responsibility to protect your business from a cyber security attack, the consequences are severe:

- *61% of cyber-attacks target small business with 1,000 employees or less[1]; and*
- *60% of small companies go out of business within 6 months of a cyber attack.[2]*

And if you are thinking that you are too small to be noticed by hackers, think again.

> *According to the security company Symantec, cyberattacks on small businesses rose 300 percent in 2012 from the previous year.[3]*

---

[1] "Verizon Data Breach Investigative Report." 2017.
[2] "CYBER SECURITY STATISTICS – Numbers Small Businesses Need to Know." 1/3/2017, Matt Mansfield, *Technology Trends,* https://smallbiztrends.com/2017/01/cyber-security-statistics-small-business.html.

[3] "Why Your Business Might Be a Perfect Target for Hackers." *Inc.* Magazine, John Brandon, 12/2013/1/2014. https://www.inc.com/magazine/201312/john-brandon/hackers-target-small-business.html.

THREATS

A top cybersecurity threat is the potential which exists that your company data will either be lost or stolen. Internal attacks and external attacks threaten your business. Internally, employees could accidentally place your company at risk through social engineering or human error, and alternatively could intentionally attack your computer systems, or implant sleeper code that may not be used for many months/years. Externally, experts identify nation-state attacks, ransomware, distributed denial of service ("DDoS") attacks, and the internet of things ("IoT") as the biggest cybersecurity threats of 2017.[4]

RISKS

Cybersecurity risk measures how or in what way your data will be affected by an effective cybersecurity attack. The availability of your data, integrity of your data and the confidentiality of your data are at risk from cybersecurity threats. Practically speaking, a cybersecurity attack could prevent you from accessing your own company's data, consequently bringing your business to a halt. A cybersecurity attack could affectively change or manipulate your company's data making your use of it nearly impossible, or an attacker could provide your company data to the highest bidder, your biggest competitor or the public at large. The result of these risks is collectively labelled a "data breach" or "data leakage". To be clear, a data breach which is damage to the confidentiality of your data, will cost your business time and money and lots of it. According to the Ponemon Institute Research Report, sponsored by IBM, data breaches cost more in 2016 than in 2015:

> *According to our research, the average total cost of a data breach for the 383 companies participating in this research increased from $3.79 to $4 million. The average cost paid for each lost or stolen record containing sensitive and confidential information increased from $154 in 2015 to $158 in this year's study.*[5]

To be sure the cost of a data breach depends on the type of data and amount involved, but you can easily do the rough math. Multiply the number of sensitive or confidential records your company maintains by $158 not forgetting to count your employee records (payroll systems, health records and tax information), customer lists and confidential customer records and for every 100 records lost you will pay/lose on average $15,800. But this is only the measure of 1 of the risks we are discussing. How

---

[4] "Top 5 Cybersecurity Threats of 2017." NOPSEC, 2/9/2017, https://www.nopsec.com/blog/top-5-cybersecurity-threats-for-2017.
[5] "2016 Cost of Data Breach Study: Global Analysis." Ponemon Institute, June 2016. https://www.ibm.com/security/data-breach.

much money would your company lose per day if you could not access your data? How much money would your company lose per day if your data was corrupted and not accurate? Imagine for a few minutes the loss to your bottom line if your company lost email for a week or you could not access the Internet for two weeks or your company website was incapacitated for a month. Begin to combine these damaging scenarios or to add in a data breach on top of these potential events contemplating the integrated nature of computers and data in your day to day survival and the need to protect and plan for a cybersecurity attack becomes all to obvious.

CONTROLS

Cybersecurity controls are the steps your business should take to protect its data and the infrastructure supporting it. How do you know which controls to implement? The simple answer is that your company must develop a written Information Security Program ("ISP") which incorporates policy, procedure and guidelines/standards. ISPs are sought by your regulators/examiners, insurers, investors, Board and others. Your company can complete this task even if you are starting from ground zero, and to build on the simple approach I am proposing, you only have two options. Build your own ISP or pay another company to do it for you. Whichever path the company chooses, however, your business is going to have to change.

BUILDING AN ISP

If your company chooses to build its own ISP, I suggest an approach similar to the steps any company takes to protect its physical assets. Identify and categorize company data, identify the infrastructure used to access the data, assess potential threats against data and infrastructure, measure the risks against data and infrastructure, implement controls to protect data and infrastructure and finally, prepare a plan in the event of a compromise of either data or infrastructure.

Data

First, clearly understand the asset you want to protect which is in this case your company data and customer data. Your company does not likely invest many resources in protecting its pencils, but it probably invests at least some resources in protecting machines or inventory without which it cannot do business. As with assets so with data. Not all data is created equal, and protecting all data equally is not good business sense, rather invest in protection levels commensurate with the value of the data being protected.

Infrastructure

Second, identify the infrastructure the company uses to access and benefit from its data. For example, if your data is stored on a removable storage device (disc, flash drive etc.), then you use some type of computer to access the data. By its nature data is completely useless to any company without the infrastructure to access it, and your ISP will vary depending on where your data is stored (onsite, off-site), how it is accessed (desktop, laptop, mobile device) and where your employees access the data (onsite, off-site via the cloud) and network.

Assess Threats

Your company faces a variety of external and internal threats with employees at the top of most information security professionals list, whether through intentional or unintentional acts.

The Verizon Data Breach Investigations Report ("Verizon DBIR") is a valuable summary of realized threats. In its tenth year, the 2017 edition is 76 pages long and can be downloaded at http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/. In addition, a variety of credible summaries of the Verizon DBIR are available online.[6] Based in part on the Verizon DBIR, common threats include[7],

1. DDoS Attacks[8]
2. Drive-By Downloads[9]
3. Malvertising[10]
4. Malware[11]
5. Man in the Middle Attacks[12]
6. Password Attacks
7. Phishing[13]

---

[6] "Cyberespionage and ransomware attacks are on the increase warns the Verizon 2017 Data Breach Investigations Report." 4/27/2017. http://www.verizon.com/about/news/cyberespionage-and-ransomware-attacks-are-increase-warns-verizon-2017-data-breach.

[7] "8 Types of Cyber Attacks Your Business Needs to Avoid.", QuickBooks Resource Center, Megan Sullivan, http://quickbooks.intuit.com/r/technology-and-security/8-types-of-cyber-attacks-your-business-needs-to-avoid.

[8] An attack on a computer system(s) in which a network of computers floods an online resource with high levels of unwanted traffic so that it is inaccessible to legitimate service requests.

[9] The unintended download of computer software from the Internet which is then used by an attacker to alter, disable or access systems and/or data.

[10] A term denoting "malicious advertising" which is the use of online advertising to spread malware. Malvertising involves injecting malicious or malware-laden advertisements into legitimate online advertising networks and webpages.

[11] Software intended to damage a computer, mobile device, computer system, or computer network, or to take partial control over its operation.

[12] Abbreviated as MITM, a man-in-the-middle attack is an active Internet attack where the person attacking attempts to intercept, read or alter information moving between two computers.

8. Pretexting[14]
9. Ransomware[15]
10. Rogue Software[16]

Employees subject companies to 8 of these 10 threats. In fact, the Verizon DBIR indicates that 81% of hacking-related breaches directly resulted from stolen or weak/guessable passwords.

Measure Risks

To appropriately measure risk, companies must systematically identify the assets, data and infrastructure, vulnerable to assessed threats and identify the impact of a cyber-attack. This step is necessary (1) to identify the best defense or controls to implement; and (2) to appropriately deploy those controls to defend your company's assets according to their value.

While a variety of tools are available to measure risk and a bevy of companies stand by to assist any size company in this task, I suggest that a basic approach will require your company to:

1. Identify and categorize data;
    a. Storage
        i. Onsite
        ii. Offsite
    b. Type
        i. Sensitive
        ii. Confidential
        iii. Public
2. Identify all hardware;
    a. Administrators
    b. Users

3. Identify all software;

---

[13] To try to obtain financial or other confidential information from Internet users, typically by sending an email that looks as if it is from a legitimate organization, usually a financial institution, but contains a link to a fake website that replicates the real one.
[14] A form of social engineering in which an individual lies to obtain privileged data. A pretext is a false motive. Pretexting often involves a scam where the liar pretends to need information in order to confirm the identity of the person he is talking to.
[15] Ransomware is malicious code that is used by cybercriminals to launch data kidnapping and lockscreen attacks.
[16] Rogue security software is a form of malicious software and Internet fraud that misleads users into believing there is a virus on their computer, and manipulates them into paying money for a fake malware removal tool (that actually introduces malware to the computer).

a. Administrators
b. Users

With this information, your company can measure its cybersecurity risk and begin to appropriately build and deploy controls to defend against a cyberattack.

Implement Controls

The controls a business should implement flow from the threats and consequent risks to the company. Effective controls will include decreasing the company's risk profile, training employees and hardening infrastructure.

Decreasing Risk Profile

Simply put decreasing the businesses risk profile involves limiting who can access data and limiting how the data can be accessed. Your company should only allow employees with a business need to access confidential and sensitive data. In addition, businesses should control the access points through which data can be retrieved by answering some basic questions:

1. Do my employees need to be able to access data from off-site?
2. Do my employees need to be able to access data from a laptop, mobile device or tablet?
3. Do my employees need to be able to access data through an internal wireless network?

If the answer is no to these questions then the business should deny that access, thus decreasing the overall avenues through which a cyber security attack could be launched.

Employee Training and Monitoring

Training and monitoring employees are essential controls. The 2016 Verizon Data Breach Investigations Report concluded that approximately 50% of the incidents reported were due to employee actions – miscellaneous errors, misuse of privileged access, insider collaboration, and the physical theft or loss of information from work areas, vehicles or a residence. The training should be no less than annual and on an as needed basis. Include practical guidance on strong password maintenance, how to respond to suspicious emails and standard steps for addressing onsite visitors, vendors and contractors. This training can be conducted by a well-informed employee or by a third-party. Test your employee's knowledge and responses in a real-world environment.

Monitoring takes many forms—background checks, performance reviews, monitoring changes in behavior and social activities, both before hiring and throughout employment. Control what employees may access and ensure proper password controls. Other low-cost controls including walking through the office to identify whether any computers are left unattended and unlocked or whether passwords are written down and visible. Finally, businesses can also hire third-parties to conduct testing of employees. StaySafeOnline.org provides several additional resources for employee training as do a variety of other organizations.

Infrastructure Hardening

Infrastructure hardening is the process of strengthening your cyber security defenses by fine tuning and maintaining both hardware and software. A variety of online resources exist and are included below to guide businesses on this subject, but the basics include:

1. Develop a Hardware and Software Inventory;
2. Create Server and workstation standard configurations;
3. Perform Regular Patch Management;
4. Implement automated anti-virus and anti-malware software;
5. Use firewalls;
6. Backup and encrypt files and disks;
7. Turning off unused features of software/hardware;
8. Removing unused programs;
9. Changing default passwords for software/hardware;
10. Requiring the use of strong passwords; and
11. Performing regular software/firmware updates.

Incident Response Plan

Each of the issues outlined above are designed to prepare your business to win the cyber-security battle. But, what if you lose despite your best efforts? Any business should have an Information Security Incident Response Plan ("IRP").

> *The goal of the Computer Security Incident Response Plan is to detect and react to computer security incidents, determine their scope and risk, respond appropriately*

to the incident, communicate the results and risk to all stakeholders, and reduce the likelihood of the incident from reoccurring.[17]

This document is meant to be a practical battle plan identifying who is responsible for each step in the plan, what everyone will do, how they will do it and when they will do it. Once documented, the IRP should be tested in a table-top exercise simulating a potential cyber-attack. In addition, it is best practice to audit your vendor's compliance in this area.

Vendor Management

If your company utilizes a third-party to manage, store or process data or utilizes a third-party to build, maintain or manage infrastructure, you should build a vendor management program which identifies your company's requirements for how that third-party handles your data and your infrastructure. This is best accomplished in two steps-Due Diligence and Contract Negotiation. Before engaging the third-party, require the third-party to provide proof that they both have and implement a comprehensive ISP and IRP. The ISP and IRP should meet your business's standards and be tailored to the specific services the third-party provides your business. Finally, ensure the contract clearly identifies that these requirements are ongoing obligations, the neglect of which will result in a breach and potential money damages.

Cyber Security Insurance

Your company should strongly consider obtaining Cyber Security coverage as general liability insurance no longer typically covers such incidents.[18] The services provided by such policies vary greatly depending on your size, the maturity of your ISP and the type of data your business maintains. In choosing an appropriate policy, consider your business model. A web based service company will require different insurance than a financial institution.[19]

Law Enforcement

Both in preparing your businesses ISP and in planning the company's IRP, participate with law enforcement. Generally, the Department of Homeland Security, the FBI and the U.S. Secret Service will

[17] "Computer Security Incident Response Plan." Carnegie Mellon University, https://www.cmu.edu/iso/governance/procedures/docs/incidentresponseplan1.0.pdf
[18] "5 Tips for Clients to Consider When Buying Cyber Liability." 11/17/2014, David Lewison, http://www.insurancejournal.com/magazines/features/2014/11/17/346566.htm.
[19] "Buying Cyber-Insurance: 5 Tips." 9/2/2014, Jeffrey Roman, Bank Info Security, http://www.bankinfosecurity.com/cyber-insurance-a-7250.

make available tools and in some cases individuals that will assist in employee training and in responding to a data breach. Remember, your data is an asset and theft of it is quite likely a crime. Each of these organizations can be an asset to your organization in the event of a data breach, but to best utilize their resources, establish communication before your company experiences a data breach so that you can efficiently make contact when you do experience a data breach.

In addition, organizations like the National Cyber-Forensics & Training Alliance can serve as a conduit between law enforcement and private industry to communicate knowledge regarding potential cyber-attacks and valuable forensics regarding attacks which have already taken place.[20]

CONCLUSION

Cyber-security criminals are using every tool at their disposal to target your company. Is your company taking advantage of all the resources which are available to defend against an inevitable cyber-attack?

Identify the threat. Measure the risk. Implement controls. Inexpensive tools and free resources are available to your company which will protect it from the financial, reputational, legal and physical losses that result from the reality of cyber-security attacks.

[20] www.ncfta.net