White Paper

THE TOP TEN CYBER RISKS

Facing Small and Medium-Sized Businesses (SMBs)

October 2015

CyberIntegrity

THE TOP TEN CYBER RISKS FOR SMBs

Reports of massive data breaches now appear in the headlines on a regular basis. Owners, partners, administrators, and CEOs, in organizations of all sizes, are taking notice and beginning to ask questions. Fewer now assume that their companies are too small to be targets. Leaders want to understand their overall cyber risk exposure but may not know where to start.

This white paper addresses the top ten cyber risk areas for small and medium sized businesses or professional corporations. Specific risk profiles vary greatly from firm to firm. Each of these will not apply equally to every company. However, experience and industry data highlight these as the most common cyber risk areas. Understanding these risks is the first step in developing a plan and focusing resources and attention where it matters most.

This white paper ends with recommendations for addressing cyber risk in an economically feasible way. Budgets and person-hours are limited. Firms need strategies to reduce risk without diverting key people from their main responsibilities and without breaking the bank.

#1 Direct Monetary Theft

Unlike personal bank accounts, business accounts are not protected from unauthorized withdrawals and other fraud. One company that found this out the hard way is Tennessee Electric Corporation (Now TEC Industrial). The computer they used to upload payroll files to their bank was compromised with malware. The hackers then substituted a fake payroll file to TEC's bank. Before this was discovered the hackers used money mules to withdraw $372,804. This relatively small company ultimately lost $192,656 not including the effort and resources expended on the portion recovered.

TEC Industrial is not alone. The State of California closed Efficient Services Escrow Corp after hackers stole more than $1.5 million from their escrow accounts. Choice Escrow of Mississippi lost $440,000 in a similar manner. Even larger companies are susceptible. Scoular, a $6B agricultural supply chain company lost $17 million when impostors used fake emails to direct unsuspecting employees to create fraudulent wire transfers. Scoular simply absorbed that loss in a way most smaller companies could never afford.

Not every organization holds funds in escrow but every company maintains at least one bank account. For this reason, and because of the potential financial impact, this type of theft ranks first among cyber risk areas for small and medium businesses.

#2 Cyber Extortion

In one five month period, 625,000 businesses and individuals were hit with a single version of "ransomware". Ransomware systematically accesses every file on an infected computer, scrambles them, and renders them unreadable by the legitimate owner. In business settings, the impact is much worse in that ransomware will encrypt every file it can access on the network. Within a short period of time, one infected computer can essentially wipe out all the data in an entire company.

The perpetrators of this malware are counting on victims to pay a ransom for the decryption key to unscramble their files. A typical ransom demand is for $200-$500 in Bitcoin but some victims have paid as much as $10,000. What's worse, paying the ransom does not guarantee full recovery or that the bad guys won't come back for more.

Antivirus (AV) software is only partially effective against ransomware. The hackers modify their versions continuously to avoid detection. AV vendors quickly update their signature detection but that can be too late if your business is hit on "Day Zero".

2475 Northwinds Parkway, Suite 200 • Alpharetta, Georgia 30009 • www.CyberIntegrity.com
Phone (404) 783-1348 • Email: info@CyberIntegrity.com

CyberIntegrity

#3 Exposure of Client / Customer Information

Most of the highly publicized stories we see about cybersecurity breaches involve theft of millions of credit card accounts, health records, employment data, or other personal information. Most also involve large corporations or government agencies. The incidents at Target, Home Depot, Anthem Blue Cross, and the Office of Personnel Management are prominent examples.

Unfortunately, these high profile examples are but the tip of the iceberg. Over 500 new breaches of customer/client/employee data are reported every month and the vast majority of these are of compromised SMBs. Worse, the number of reported breaches pales in comparison to the number of unreported breaches. By some estimates, 94% of all detected breaches are never made public. This implies over 8000 new cases every month.

Over 500 new breaches of customer / client / employee data are reported every month

Here's the good news: organizations that perform a thorough risk analysis and take reasonable measures to secure their environments are less likely to be victims of a security breach. The cybersecurity version of locking windows and doors, installing a home monitoring system, and providing a well-lit environment does, in fact, go a long way. Large companies, government agencies, or other entities that provide rich targets to sophisticated criminals or state actors won't be protected by these basic precautions but the vast majority of SMBs will.

#4 Damage to Reputation / Trust

Exposing confidential client information is one way to damage relationships but it isn't the only way:

- Imagine the impact to your organization if your website was suddenly defaced with inappropriate language and/or images.
- How much damage control would be required if computers inside your company had been, unbeknownst to you, commandeered to generate attacks against others?
- What if visitors to your website became infected with malware they caught by visiting your site?
- Consider the consequences if parties clicking on your company in Google search results landed on a rogue site instead.

Each of these scenarios, and many others, play out daily in the real world.

Most of these attacks succeed because basic precautions haven't been taken and because SMBs simply aren't aware of their susceptibility. Some endure for weeks, months, or even years without detection. Compromises such as these are more indirect in that company resources are being subverted for nefarious purposes. Unfortunately, the damage to an organization's reputation can be quite impactful.

#5 Fines/Settlements

After suffering security lapses, numerous companies have been hit with fines or compelled to pay financial settlements. The US Department of Health and Human Services' Office of Civil Rights (OCR) is among the most aggressive enforcement agencies. In one case, a small hospice paid $50,000 to settle after a single laptop with fewer than 500 patient records was stolen. On the extreme, settlements with OCR have reached as high $4.8 million.

CyberIntegrity

Healthcare is by no means the only sector facing possible fines or settlements. The Federal Trade Commission has increased the number of cases filed against businesses every year since 2010. No industry is immune. Retail and wholesale, consumer and business services, utilities, financial services, transportation, and manufacturing entities have all settled cases with federal and state agencies … and paid penalties.

#6 Business Continuity Loss

Hackers commonly bring down ecommerce and informational sites by overwhelming them with traffic. Motives can be political, cyber-vigilantism (retribution for some perceived wrongdoing by the targeted company), extortion (an attempt to collect ransom to make the attack stop), or simply for the entertainment or ego of the attacker. These "denial of service" attacks are common and increasing but the average SMB is unlikely to ever experience one.

Far more common, however, is business continuity loss because of some technical failure. These failures are caused by server crashes, network outages, incorrect configuration changes, component malfunctions and a myriad of other reasons.

When evaluating risk, it is important to consider a.) what would happen to your business if critical systems were unavailable for an hour, a day, or longer , b.) where are the weak spots and single points of failure in your environment and c.) what can and should be implemented to guard against loss of business continuity.

#7 Damage to Competitive Position

When hackers steal customer health records, credit cards, and other personal information, corporations are required to disclose the breach. For that reason we tend to hear about those incidents frequently. Less commonly heard, but potentially more damaging, is theft of trade secrets, intellectual property, product pipeline data, and client/prospect lists.

The reports we do see about stolen proprietary information tend to implicate entities in China which may have the tacit approval of the Chinese government. As sinister as that may be, most SMBs are at much higher risk from a more pedestrian threat: insiders. Current employees do become ex-employees and often go to work for a competitor. Although the vast majority of employees are honest, the opportunity is abundant and the likelihood of detection is low. 59% of companies recently surveyed said they have no way of detecting insider data theft.

59% of companies recently surveyed said they have no way of detecting insider data theft.

#8 Legal Liability / Cost of Defense

A clear pattern has emerged. In the aftermath of a high profile data breach, the company suffering the breach faces a class action lawsuit. This has been true with Sony, Target, Neiman Marcus, Experian and many others. Today, SMBs are less likely defendants in these class action cases. However, that risk is increasing as law firms develop specialized practices dealing with cybersecurity breaches.

Potential liability extends well beyond the scenario of exposing customer data. Consider, for example, a situation where hackers compromise your systems then use your access to a partner system to exploit that partner. This was the case with Fazio Mechanical Services whose access to Target's systems was the original entry point for their massive breach.

CyberIntegrity

#9 Loss of Data Integrity

When discussing cybersecurity we tend to focus on safeguarding *confidentiality*. Earlier in this white paper we also emphasized the *availability* of information (see #6 Business Continuity Loss). Often what is forgotten is the third leg of the cybersecurity triad: *integrity.*

Most organizations depend on the accuracy of the data they use and manage. In some industries, if data were to be modified for nefarious purposes, it would subvert the entire mission. In the education field, for example, there are numerous examples of students hacking into school systems to change grades. On the other end of the spectrum, the Director of National Intelligence recently warned that data manipulation was the next phase of cyber warfare. In assessing risk, all organizations should consider how bad actors (internal or external) might try to gain advantage by modifying data.

10 Business Closure

For SMBs without deep pockets a significant data breach can be fatal to the business itself. A study by the National Cyber Security Alliance found that 60% of small firms go out of business within 6 months of a data breach. Efficient Services Escrow Corp is an example mentioned earlier in this white paper. Another is CodeSpaces, a technology firm, which was forced to close its doors following a prolonged cyber extortion attack. Clearly the stakes are high with some businesses paying the ultimate price for a breach.

A Path Forward

If this list seems daunting, take heart. Organizations that pay attention to cyber risk can dramatically lower their risk profile without spending money on expensive, cutting edge technology.

The high level roadmap involves:

1. **Understanding the risks that APPLY TO YOUR BUSINESS.** There are literally thousands of threats out there but the only ones that matter are those that a.) bear a reasonable likelihood of affecting your organization or b.) would have a significant impact.

2. **Determining the best risk treatment options.** Technology is often an answer but is not a panacea. Some technology, frankly, costs more than the risk it is intended to mitigate. Policy and process can help but need to be balanced against other business imperatives. Insurance is often an effective risk transfer mechanism but pay attention to what a policy specifically covers. For certain low impact areas, it may make more sense for an organization to simply accept the risk.

3. **Educating all employees and associates.** Awareness is always your first line of defense and employee error is the preeminent way for hackers to initially compromise an organization.

4. **Practicing good governance.** Ultimate responsibility for risk management sits with the board of directors and executive management, not the IT department. Owners, partners, and boards of directors should take an active interest in understanding the organization's risk profile and how risk is being managed.

5. **Obtaining professional help if internal expertise is not available**. In choosing a consultant for risk assessment and treatment, make sure to choose one whose methodology focuses on your specific risk profile not an inventory of your technical vulnerabilities.

2475 Northwinds Parkway, Suite 200 • Alpharetta, Georgia 30009 • www.CyberIntegrity.com
Phone (404) 783-1348 • Email: info@CyberIntegrity.com

CyberIntegrity

CyberIntegrity

The Pragmatic Approach to Security™

2475 Northwinds Parkway, Suite 200 • Alpharetta, Georgia 30009 • www.CyberIntegrity.com
Phone (404) 783-1348 • Email: info@CyberIntegrity.com

CyberIntegrity