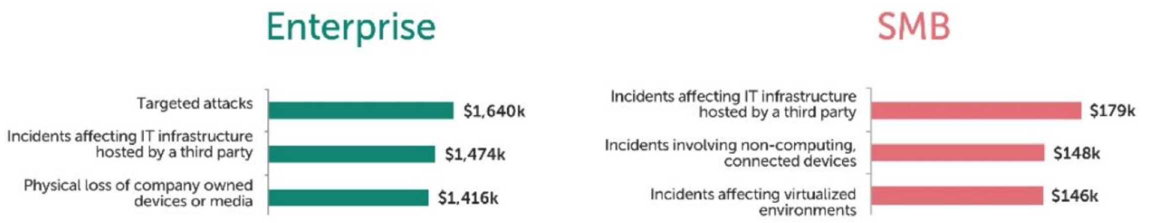
Cybersecurity is the Biggest Threat Facing Your Business Today – and You Are Not Taking the Threat Serious Enough

In today's business environment, companies must contend with a vast array of incredibly sophisticated, ever-changing cybersecurity threats. These threats target your employees and your business using hacks, social engineering, phishing attacks, and more. To keep your company protected, your Security and Compliance approach must be as sophisticated and up-to-date as the attacks of those who are trying to compromise it. Unfortunately, **company security policies are almost always less advanced than they should be**, and there are many companies where those policies are non-existent.

There is no bigger threat to your business than a cybersecurity incident, and yet we see very few companies treating this threat with appropriate levels of awareness, priority, and budget. According to a report by Kapersky Lab, the average cost of a data breach for enterprise businesses in North America is $1.6 million. If you're not an enterprise company and think you're "too small" to become a target, realize that nearly half of all cyberattacks are on small businesses, and the average cost of attacks for SMBs is $149,000 per incident.



Be truthful with yourself and consider the following:

- Is your company's security where it needs to be to protect your business, your employees, and your customers?
- Do you know what your current security posture looks like, what protections are in place, or what the procedures are should an attack be detected?
- Do you know if you are protected from the *latest* forms of cyberattacks?
- Are your employees up-to-date on recent phishing scams, and do they know what to do if they believe they have been targeted or compromised?
- Do you have the appropriate cyber-insurance in place if you are attacked and compromised?

If you're feeling a bit overwhelmed and frightened by the idea of your company's security – **good**! A bit of fear is healthy when it comes to cyber-dangers. Realize, however, that **you don't need to face this challenge alone**. Envision has been carefully watching security trends and putting in place new technologies, protocols, and services to better protect our clients. We've also created this report to help educate you on what we are seeing in the market in terms of cybersecurity.

The bottom line is this: no matter how seriously you are taking your company's security today, **you need to take it more seriously**, starting now.

In this report we will cover why:

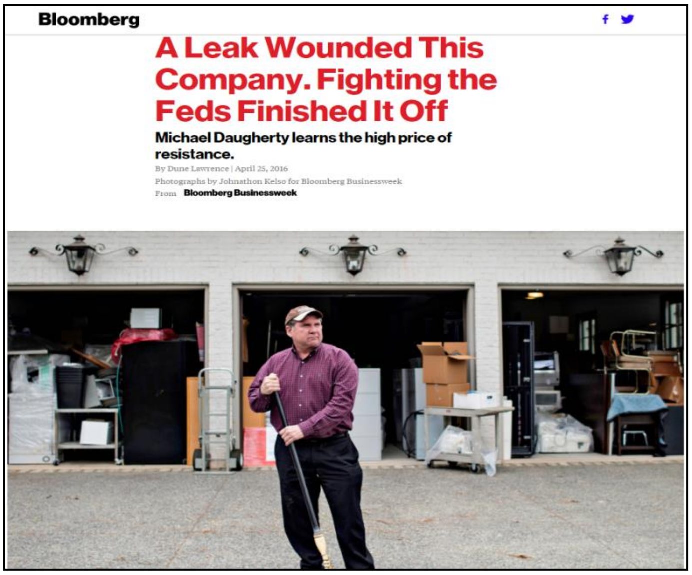
- It's Your Fault…Even if it Isn't Your Fault
- No Company is "Too Small" to Become a Target
- The Problem is Bigger Than Just Cybercriminals and Hackers
- The Impacts of an Attack Are Bigger Than You Can Imagine

Finally, we will look at A Path Forward, including the protections that we are recommending all companies have in place as part of a comprehensive approach to cybersecurity.

It’s Your Fault…Even if it’s Not Your Fault

Victims of most crimes – burglary, mugging, carjacking, theft – inspire sympathy and support, which is right and appropriate. However, if your business is the victim of a cyberattack, wherein your client or patient data is compromised, you will not get much sympathy. Rather, you may be labeled as careless and irresponsible, and your company’s reputation will suffer a serious blow.

If the incident is significant enough, your company may even be investigated and questioned about what you did to prevent the attack from happening. If the answers you provide are not adequate, your company may face significant fines and lawsuits, even if you had some protections in place. Claiming ignorance is not an acceptable defense when it comes to cybersecurity, and this potentially reputation-destroying nightmare will land squarely on your shoulders if you are compromised.



Bloomberg

A Leak Wounded This Company. Fighting the Feds Finished It Off

Michael Daugherty learns the high price of resistance.

By Dune Lawrence | April 25, 2016

Photographs by Johnathon Kelso for Bloomberg Businessweek

From Bloomberg Businessweek

Consider the story of Michael Daugherty, former CEO of LabMD. His small, Atlanta-based company tested blood, urine, and tissue samples for urologists – a business that was required to comply with federal rules on data privacy as outlined in the Health Insurance Portability and Accountability Act, or HIPAA.

LabMD had an internal IT team in place that Michael believed was protecting them from a cybersecurity incident– yet the manager of his billing department was able to download a file-sharing program to the company’s network to listen to music. Using this software, she unknowingly left her documents folder (which contained over 9,000 patient files) open for sharing with other users of the peer-to-peer network. **This was a simple, innocent mistake made by a tenured, honest employee.** Unfortunately, this vulnerability was not caught by the IT department, and the company’s data was left unprotected.

In a strange twist to this story, LabMD was not compromised by a hacker or cybercriminal, but rather by an IT services company. This company gained access to the data file and tried to use it to extort LabMD into hiring them for their security services. When Daugherty refused to hire the company and use their services, they reported him to the Federal Trade Commission.

After filing some 5,000 pages of documents to Washington, LabMD’s CEO was told that the information he shared on the situation was “inadequate”. In-person testimony by the staff regarding the breach was requested. They also asked for more details on what training manuals he had provided to his employees concerning cybersecurity and they wanted documentation on firewalls and the penetration testing that was done at his company.

In the end, LabMD's employees began to leave the company, looking for more secure jobs at organizations that weren't under investigation. The company's sales steeply declined as clients took their business elsewhere, and LabMD's insurance providers refused to renew their policies.

LabMD eventually closed their doors as the FTC relentlessly pursued Michael Daugherty with additional demands for documentation, testimonies, and other information. These requests ate up countless hours of time, leaving an emotional strain and a financial burden on the one-time owner of this small company. Once again, all of this was because an employee innocently downloaded software to listen to music while at work. Even though security protocols were in place, they were insufficient, leading to:

- Private data entering the wrong hands
- Legal ramifications, including significant fees for defense lawyers, based on the data breach
- Loss of reputation with clients, leading to loss of business from those clients
- Loss of employees due to shaky company standing in the wake of the investigation
- The eventual closure of the business

You may have great people at your company whom you trust and respect, but could you see one of them making an innocent mistake like this one? Can you imagine one of them downloading software to do their job and unknowingly introducing malware into your network or opening up a vulnerability to your data? Good employees can make mistakes, and those mistakes can cost you dearly.

No Company is "Too Small" to Become a Target

As we have just seen in the example of LabMD, there is no such thing as being "too small a company" for cyberattacks. In fact, cybercriminals want you to believe that you are too insignificant to be worth their time. That makes you easy prey because it lulls you into a false sense of security, causing you to put few, if any, protections in place to keep those criminals at bay.

The harrowing truth is that, according to research by Panda Security , 230,000 NEW malware threats are being released every single day, and **nearly half of the cyberattacks occurring are aimed at small businesses**. You may not hear about all these attacks because the news tends to report on bigger incidents with more of a national or global impact, but make no mistake – small, "average" businesses are being compromised daily. Clinging to the misguided ignorance of "that won't happen to me" is a surefire way to leave yourself wide open to these attacks.

This is according to research from Panda Security, estimating Trojans to be the main source of malware — being responsible for about **51.45** percent of all malware

The National Cyber Security Alliance reports that **one in five small businesses have been victims of cybercrime in the last yea**r – and that number includes only the ones that were reported. Most small businesses are too embarrassed or afraid to report an incident, fearing the bad publicity and financial impact of publicly acknowledging that incident. It's therefore safe to assume that the true number of SMB-focused cyberattacks is far higher than the reported number.

Still think you're "too small" to need to be prepared for a cyberattack? Ask yourself these questions:

- Are you "too small" to be significantly damaged by a ransomware attack that locks all your files for several days or more?

- Are you "too small" to deal with a hacker using your company's server as "ground zero" to infect all your clients, vendors, employees, and contacts with malware?

- Are you "too small" to worry about someone taking your payroll out of your bank account?

According to Osterman Research, the average small business hit by a cyberattack loses over $100,000 per ransomware incident and experiences over 25 hours of downtime (Note – this is actually a bit lower than the $149k/per incident loss found in similar research by Kapersky Lab). A loss of $100k to $149k, while certainly significant, may not be enough to sink your company, but what about the bad publicity, loss of trust from your client base, or the loss of faith from your employees? Those are all residuals that could be costlier to your business in the long run than the initial loss from the attack. The bottom line is that NO organization is "too small" to become a victim of a cyberattack, which means that NO company is "too small" to take cybersecurity seriously and deploy the necessary measures to protect themselves.

The Problem is Bigger Than Just Cybercriminals and Hackers

Do a Google Image Search for “hacker” or “cybercriminal” and you will find lots of pictures of shady individuals in black hooded sweatshirts bent over a laptop – but this is not the only face of cybercrime that your company needs to worry about.

Many businesses erroneously think cybercrime is limited to hackers based in China or Russia, but the evidence is overwhelming that disgruntled employees, both from your company and from your vendors, can cause significant losses due to their knowledge of your organization and access to your data and systems. How can they hurt your company?

- Employees leave the company with proprietary files, client data, and confidential information stored on personal devices, as well as retaining access to cloud applications, such as social media sites and file-sharing sites (Dropbox or OneDrive, for example) that you aren’t even aware they were using.

- According to an in-depth study conducted by Osterman Research, 69% of businesses experience data loss due to employee turnover, and 87% of employees who leave a company take data with them. What do they do with that information? Sell it to competitors, become a competitor, or retain it to use at their next job.

- Disgruntled employees can DELETE everything on their way out the door. Here’s a scenario that is sadly all too common: An employee is fired or quits because they are unhappy with how they are being treated, but before they leave, they permanently delete ALL their e-mails and any critical files they can get their hands on. If you don’t have that data backed up, **you will lose it.**

- Former employees can anonymously share private company information online. This could be anything from trade secrets to unflattering emails and other information. Many experts believe that the infamous Sony Pictures hack in 2014, which has been widely blamed on North Korea, was actually an inside job. While the FBI has rejected these claims, the reality is that the leak *could* have come from current or former employees who had access to the data that was leaked.

There’s also the threat of vendor theft. Your payroll, HR, and accounting firms have direct access to highly confidential information and a unique ability to commit fraud. Their employees, not just the leadership team, can steal money, data, and confidential information. All it takes is a part-time employee – perhaps hired to assist during a busy period and who is not being closely supervised or is working from home on routine tasks with your account - to decide to make a little money on the side by selling data or siphoning funds from your account.

There is no doubt that there are foreign cybercriminals targeting companies like yours, but they aren’t the only threat you must guard against. A compromise is a compromise, whether it comes from outside your organization, or from someone inside who has trusted access to your sensitive data. Your job is to ensure that **you are protected from both potential attack vectors**.

The Impacts of an Attack Are Bigger Than You Can Imagine

Throughout this whitepaper, we have mentioned some of the impacts of cyberattacks, but let's take a deeper look at what will happen to your company if you are not prepared for an attack:

1. **Reputational Damages:** What's worse than a cybersecurity incident? Trying to cover it up. Companies like Yahoo! are learning that lesson the hard way, facing multiple class-action lawsuits for *not* telling their users immediately when they discovered they were hacked. With Dark Web monitoring and forensics tools, *where* data gets compromised is easily traced back to the company and website, so you cannot hide it.

   If your clients' data is compromised, they will demand answers. They will want to know what protections you had in place and how those protections failed. You certainly do not want to reply with, "Sorry, we got hacked because we didn't think it would happen to us" or "We didn't want to spend the money on the necessary security."

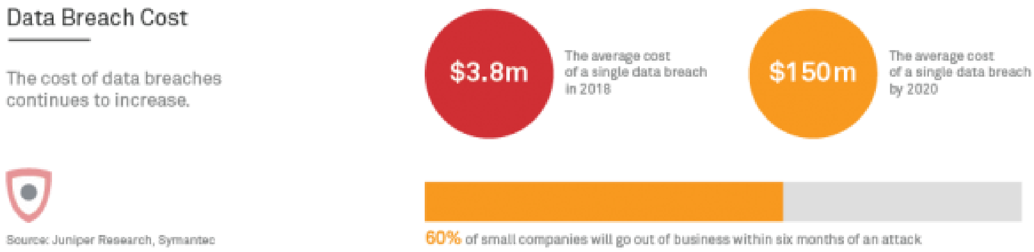
2. **Government Fines, Legal Fees, Lawsuits:** Breach-notification statutes remain one of the most active areas of the law. Right now, several senators are lobbying for "massive and mandatory" fines and more aggressive legislation pertaining to data breaches and data privacy. The courts are not in your favor if you expose client data to cybercriminals.

   Once again, don't think for a minute that this applies only to big corporations – **any small business that collects customer information also has important obligations** to tell their customers if they experience a breach. In fact, 47 states and the District of Columbia each have their own data breach laws – and they are getting tougher by the minute.

   If you're in healthcare or financial services, you have additional notification requirements under the Health Insurance Portability and Accountability Act (HIPAA), the Securities and Exchange Commission (SEC), and the Financial Industry Regulatory Authority (FINRA). Among other things, HIPAA stipulates that if a health care business experiences a breach involving more than 500 customers, it must notify a prominent media outlet. SEC and FINRA also require financial services businesses to contact them about breaches, as well as any state regulatory bodies.

3. **Cost, After Cost, After Cost:** One cybersecurity incident, one ransomware attack, or one rogue employee you are not protected against can create hundreds of hours of extra work for staff who are already maxed out when things are going well – and those hours are just the start of the costs directly related to this attack. There's also the business interruption and downtime, and backlogged work delivery for your current clients. There's the forensics costs to determine what kind of hack occurred, what part of the network is/was affected, and what data was compromised. Next, you will have emergency IT restoration costs for getting you back up and running, if that's even possible. Then there are legal fees and the cost of legal counsel to help you respond to your clients and the media. Cash flow will be significantly disrupted, and budgets will be blown up. Some states also require companies to provide one year of credit-monitoring services to consumers affected by an incident, and more are following suit.

According to the Cost of Data Breach Study conducted by Ponemon Institute, after factoring in IT recovery costs, downtime, fines, and legal fees, the average cost of a data breach is $225 per record compromised. How many client records do you have? How many employee records? Multiply those numbers by $225 and you'll start to get a sense of the costs to your organization.



Source: Juniper Research, Symantec

4. **Bank Fraud:** If your bank account is accessed and funds are stolen, **the bank is *not* responsible for replacing those funds**. Take the story of Verne Harnish, CEO of Gazelles, Inc. and author of the best-selling book *The Rockefeller Habits*.

   Harnish had $400,000 taken from his bank account when hackers were able to access his PC and intercept e-mails between him and his assistant. The hackers sent an e-mail to his assistant asking her to wire funds to 3 different locations. It didn't seem strange to the assistant because Harnish was then involved with funding several real estate and investment ventures. The assistant responded in the affirmative, and the hackers, posing as Harnish, assured her that it was to be done. The hackers also deleted Harnish's daily bank alerts, which he didn't notice because he was busy running the company, traveling, and meeting with clients. That money was never recovered, and the bank never assumed responsibility.

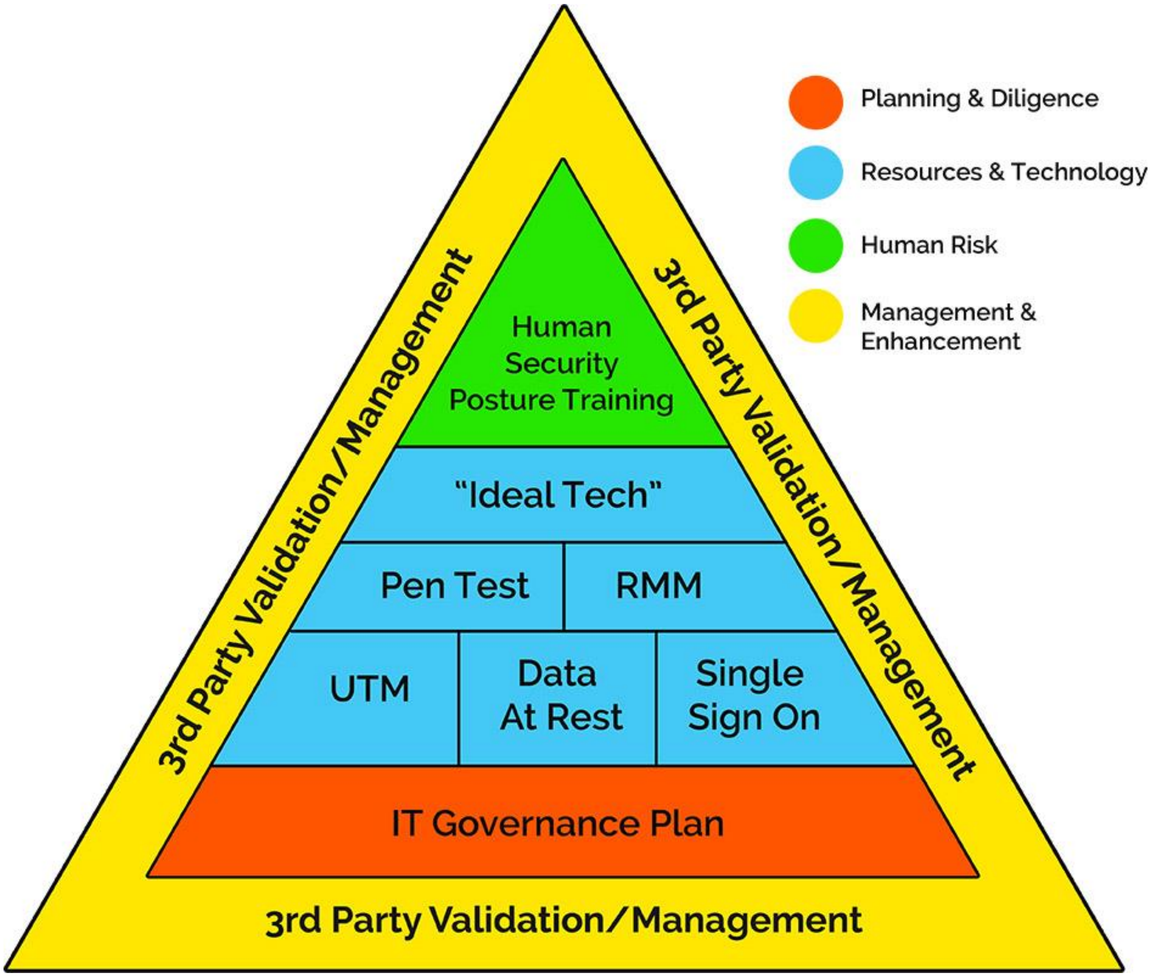
   Everyone wants to believe "not MY assistant, not MY employees, not MY company" – but do you honestly believe your staff is incapable of making a single mistake? Nobody thinks they will be in a car wreck when they leave the house every day, **but you still put the seat belt on**. You may not expect to be in a life-threatening crash, but that's not a reason to not buckle up.

5. **Using YOU as The Means to Infect Your Clients:** Some hackers don't lock your data for ransom or steal money. Rather, these cyber criminals use your server, website, or online profile to spread viruses and compromise other PCs. Hackers can use your website to relay spam, run malware, build SEO pages, or promote their religious or political ideals.

   No company wants to become the platform from which criminals can launch attacks or where zealots can spew their vitriol, but if you are not protected from cyberattack, that is exactly what could happen.

A Path Forward: How to Approach Your Company’s Cybersecurity

As we said at the start of this report, **no matter how seriously you are taking your company’s security today, you need to take it more seriously** - starting now. While every company’s security strategy will be different, our approach is represented by our “Security Triangle”:



A solid plan for your company’s security goes beyond just technology. It also includes the solid foundation of a comprehensive IT Governance Plan, as well as Human Security Posture Training to address the “human risk” in your organization. All of your security processes and policies are wrapped within 3rd Party Validation and Management services.

As part of this plan, the following are solutions that we are recommending for all companies:

- **Security Assessment** –Before you can move forward with a security strategy tailored to your specific requirements, you need to understand where you are today. A comprehensive security assessment should be the start of your engagement.

- **Employee Security Posture Training** – Your employees are of the first line of defense when it comes to security, since they are your company's biggest attack vector. To keep your company secure, they must understand the mechanisms of spam, phishing, spear-phishing, malware, and social engineering and be able to apply this knowledge in their day-to-day jobs. We recommend a customized training plan based on your specific needs, conducted through face-to-face trainings that will make complex concepts easily understood by even the least technical of your employees.

- **Multi-Factor Authentication** - We recommended multi-factor authentication for access to all critical data and applications.

- **Proactive Monitoring, Patching, and Security Updates** – Keeping your systems up-to-date with the right security patches is essential. It is also something that can be incredibly time-consuming for your internal IT staff if you do not have a concise and informed plan for managing these assets. A proactive approach that takes advantage of automation and proven processes is the best way to keep your systems updated accordingly.

- **Managed Threat Protection Services** - Creating a new layer in your security stack, this solution combines automated collection tools with expert analysis, hunting down and eliminating threats that may have slipped past other layers of protection.

- **Endpoint Encryption**- All endpoints should include solutions to make data unreadable to unauthorized users.

- **Mobile Device Management** – All mobile devices in your organization should include tools where they can be remotely monitored, managed, and locked or wiped if they are lost or stolen.

- **Insurance Review** – Cyber liability insurance can be very confusing. Depending on your plan, you may not be covered for certain incidents, or your coverage may differ from what you think it is. We recently heard an insurance specialist relate the story of a company that was breached, losing a few thousand records in the process. Their insurance plan had a deductible of $1,000 per incident, but when they went to file a claim for the breach, they discovered that the fine print of the contract stated that each record lost was considered a separate incident. This meant their deductible was actually $1000 **for every record lost** – adding up to millions in the deductible alone! They did not expect this when they purchased the insurance plan, but this story illustrates exactly why you should do an annual review of your cyber liability insurance to ensure that it's providing the right coverage for your business.

- **Ongoing Reviews and Training** – To maintain security over time, you should have a regular schedule of security reviews conducted by third party. Your staff should also consistently train on the latest scams and vulnerabilities to ensure that security posture is maintained as new threats emerge in the industry.

Are You Ready to Get Serious About Security? We Can Help.

This list may seem daunting, but as part of a comprehensive, strategic security plan, it is absolutely something your company can accomplish. As we've seen In this report, failing to maintain a high level of security can have devastating impacts on your company.

Envision's security experts have worked with companies of all sizes across a variety of verticals and we can help you secure your company.

Contact the Envision team today and let our security experts show you how we can better protect your company, your people, your clients, and your overall peace of mind.

About Envision Technology Advisors

Founded in 1998, Envision Technology Advisors provides a range of business and technology consulting services to the New England area and beyond. Envision's specialties include cloud and managed services, desktop and data center virtualization, network and infrastructure consulting, business continuity & disaster recovery, cybersecurity consulting, data services, and digital communications and design. With offices in Pawtucket, RI, the Greater Boston area, and Nashville, TN, the company has been named a "Best Place to Work" for ten straight years. For more information, visit http://www.envisionsuccess.net.