Detect and Prevent Cybersecurity Threats to Your Business

DIAMOND IT
your potential. our passion.

Cybersecurity has become a major priority for more than just large corporations.

Experienced hackers and sophisticated phishing schemes have affected all organizations, regardless of size. Consider this alarming statistic — **60% of small businesses go out of business within six months of an attack**. You might want to read that again. That is higher than a coin flip chance of not surviving.

So how does the average small business stand a chance of protecting against constantly evolving threats?

Setting up a strong defense now is critical to avoiding big issues in the future. By implementing preventative monitoring, using the latest information to update and perfect your defenses and having a partner who is well versed in the latest technologies helps protect your organization from network exploits, malware and advanced attacks.

This eBook offers the information you need to detect and prevent cybersecurity threats to your business. This includes alarming security statistics that tell the truth about today's security landscape, how to detect your company's level of risk, a test to assess your current threat level, must-have tools in your security arsenal and a discussion on the benefits of cybersecurity insurance.

CONTENTS

Your 5 Most Common Ways to Get Breached

Cyberattacks rightfully cause fear in small and large businesses alike, and recent statistics show no one is safe.

1. Malware, Viruses, Spyware, Ransomware — While each one of these types of potential attacks may have its own objective, gaining access to your most sensitive data is almost always the intended result. Any introduced malware has the potential to lock down your systems, gain access to confidential data or erase all the information on your hardware.
2. Phishing — Ranked as one of the most common types of attacks, phishing is a hacking technique where thousands of emails are sent out with a link or attachment that replicates commonly visited websites. Once the user clicks on the link, opens the attachment or enters any data, the hacker gains access to all the data and information on the user's system.
3. Distributed Denial of Service (DDoS) — Nexusguard, an internet security specialist, reported that DDoS cyber-attacks using domain name server (DNS) amplification tactics spiked an astronomical 357 percent year-over-year in Q4 2017. DDoS attacks serve to shut down an entire site or system by overloading it with requests and traffic that are impossible to handle all at once. Slowly getting overwhelmed, the system finally crashes and your ability to operate your business goes down with it.
4. Brute Force Cracking — This trial-and-error hacking technique is used to gain access to password-protected information by continuously "guessing" until the correct password is found. Sophisticated algorithms and software programs scour hundreds of number and word combinations simultaneously to try and crack your password.
5. Keylogger — Seemingly simple in nature, hackers use keylogger attacks to track and record keystrokes. This includes user names and passwords for protected sites and confidential portals. Keylogger targets both hardware and software and can capture strokes within a program or through a connected keyboard or smartphone.

MALWARE ATTACK FREQUENCY

Reference: www.secplicity.org/threat-landscape by WatchGuard Threat Lab (Dynamic Statistics)

Every Day

205,073

Every Hour

8,545

Every Minute

142

Every Second

2

Identify Your Risk of Being Breached — Statistics to Know

Despite what might seem like an intuitive strategy, top executives don't always understand the need for constant proactive security attention. Fear of an attack doesn't often incite a bigger investment in the IT budget because many assume the current anti-virus/firewall tools in place are "enough."

Let the statistics speak for themselves

According to WatchGuard:

- The Americas make up for 24.92% of all international malware attacks. (Seplicity)
- There are 50,647 malware attacks in America every day. That is one attack every second.

According to Small Business Trends, in 2017:

- 43 percent of cyber-attacks targeted small business.
- 60 percent of small companies would go out of business within six months of a cyber-attack.
- 48 percent of data security breaches were caused by acts of malicious intent. Human error or system failure account for the rest.
- Small businesses were most concerned about the security of customer data

Cisco 2017 Annual Cybersecurity Report

The Cisco 2017 Annual Cybersecurity Report states that ransomware is growing at a yearly rate of 350%, resulting in thousands of lost jobs and millions in financial loss.

Hiscox Cyber Readiness Report 2017

The Hiscox Cyber Readiness Report 2017 found that 53 percent of the companies assessed for cyberattack readiness were ill-prepared to deal with a cyberattack, and only 30 percent were rated "expert" in their overall cyber readiness. This confirms that most organizations are not as prepared as they should be.

Why you should worry

You're already aware of the major risks of a cyberattack, such as downtime, lost productivity and data breaches. What about some of the overlooked costs?

According to Deloitte

Deloitte writes that there are several "hidden costs" of a cyberattack that many CEOs and other key decision makers are not always aware of:

- **Insurance premiums will rise.** It's not uncommon for a policyholder to face a 200-percent increase in premiums for the same coverage after a cyber incident.
- **Loss of intellectual property.** The intangible costs associated with loss of intellectual property can lead to loss of competitive advantage, revenue and more.
- **Increased cost to raise debt.** If the credit rating of an organization drops, higher interest rates for borrowed capital always follows.

Test Your Level of Cybersecurity Preparedness

A phishing attack or a malware lockdown can cost your company thousands of dollars every day, even if your business is small. That's why it's incredibly important to be prepared.

This quick quiz will help guide your company toward an effective cybersecurity defense.

1. Are your company's critical systems backed up on an hourly or daily basis?
   ☐ Yes ☐ No ☐ I don't know
2. If your systems were hacked or otherwise compromised, do you have clean data backups?
   ☐ Yes ☐ No ☐ I don't know
3. If a network exploit occurred, can your company's data and website be restored quickly?
   ☐ Yes ☐ No ☐ I don't know
4. Are your company's critical systems accessible in the cloud?
   ☐ Yes ☐ No ☐ I don't know
5. Does your business have an emergency contingency plan in case you're the victim of a ransomware attack?
   ☐ Yes ☐ No ☐ I don't know
6. Are your employees aware of the latest security threats and how to identify them?
   ☐ Yes ☐ No ☐ I don't know
7. Is ongoing security training part of your company policy?
   ☐ Yes ☐ No ☐ I don't know
8. Are there documented procedures and an essential action plan in place if your data is breached?
   ☐ Yes ☐ No ☐ I don't know

If you responded "no" or "I don't know" to even one of these important questions, you need more tools in your cybersecurity arsenal.

Must-Have Tools for Your Security Arsenal

There is no one-size-fits all security solution, and the best protection is a constant work-in progress with a trusted partner. That said, there are must-have security tools all organizations cannot bypass if they want to maintain protection.

The following tools are the security "must haves" for any organization:

Anti-Virus — Choose a hosted anti-virus service, like ESET, that doesn't require additional server resources and is managed and monitored by an experienced IT provider. Anti-virus software scans files and computer memory for patterns that may indicate a virus infection based on the latest definitions of known viruses.

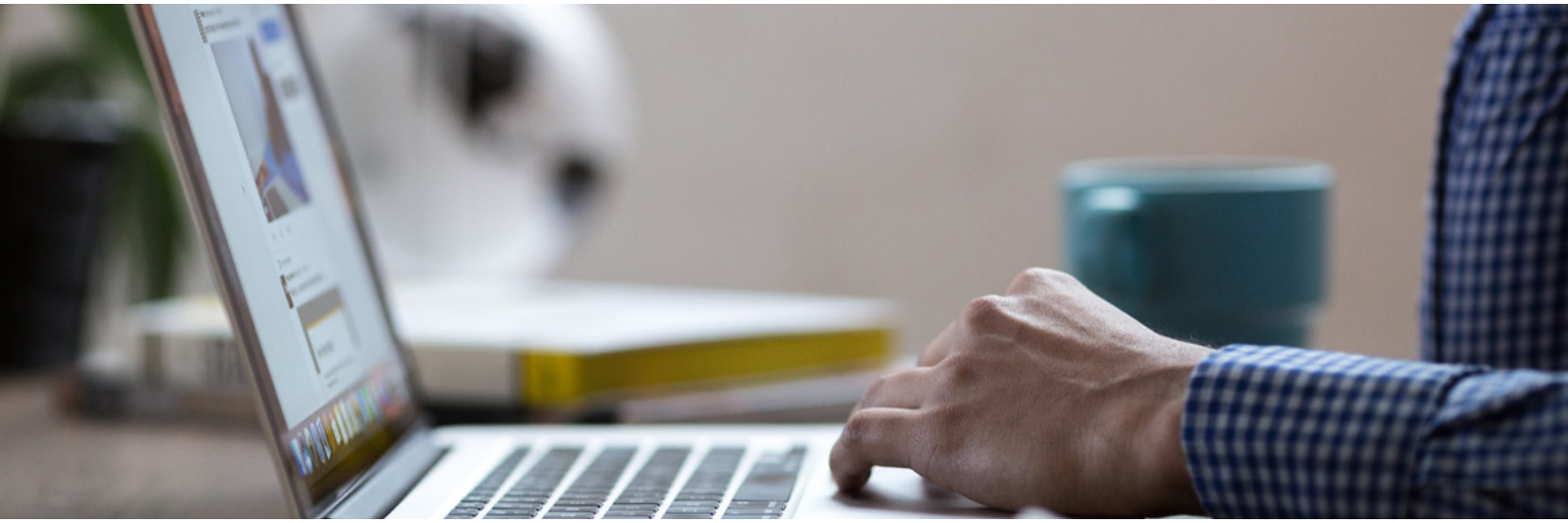
Managed Firewall — Like the firewall offered through our premier partner WatchGuard, firewalls are important for organizations of any size, serving as the protection between your internal network and the Internet. The newest firewall service provides the latest technology to protect your network from advanced threats, even while connecting to corporate data from remote locations.

Security Awareness Training — Today's employees are regularly exposed to email attacks that put businesses at risk, and training employees to recognize threats is an essential part of cyber security. Choose an IT partner who offers security training through an easy-to-use interface and includes baseline testing, ongoing training, regular phishing tests and detailed reporting so you can be sure your team is the first line of defense against IT security threats. At DiamondIT we partner with Webroot Security Awareness training services.

Annual Security Review — A thorough review of your organization's domain user accounts is critical to successful IT security, including a report of inactive users, users with remote access and domain administrator accounts. Annual security reviews include a desktop and server inventory and risk report, remote access review and external vulnerability report and IP scan.

Cloud Security — With users accessing the Internet from multiple devices in and out of the office, it is crucial to protect those devices and block access to your data before threats can reach you with tools like Cisco's CloudLock or Citrix's ShareFile solutions. Use the Internet's infrastructure to block malicious destinations before a connection is ever established.

Why You Need Cyber Liability Insurance



If you're Looking to get Insured

Cyber liability insurance is a useful tool for transferring risk as part of a sound risk management strategy. Despite the benefits, 75 percent of small businesses have no cyber risk insurance.

One deterrent may be that insurance companies require evidence of insurability, and they align your premiums and payouts to your pre-existing security postures.

Here's what you need to know to ensure you're doing everything expected to protect your cyber environment. By taking the following steps you can confidently provide evidence of insurability to qualify for the coverage you need to protect your shareholders, customers and employees.

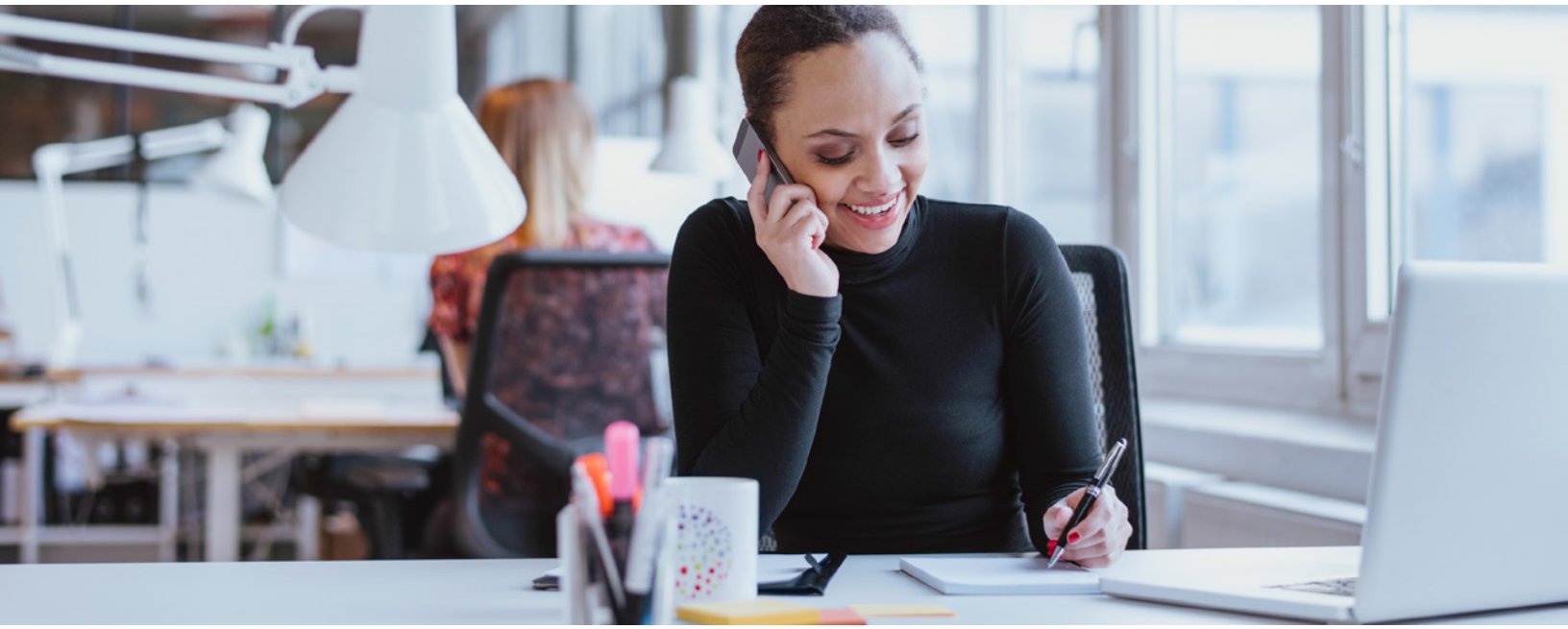
- Do not use or collect Personal Information when it's not necessary
- Identify critical data assets and protect them appropriately
- Train your staff on Information Security and Data Privacy Standards
- Implement key technologies including encryption and multifactor authentication
- Conduct regular security assessments
- Create a written incident-response plan
- Examine the processes that will produce reporting in case of an incident
- Create an actionable, written data-breach response plan that includes both internal and external communication strategies

If you are a Cyber Liability Policy Holder

If you are already covered by cyber liability insurance, it's critical to make sure you're implementing the required best practices to meet your provider's standards for coverage. Otherwise, you're liable to lose your coverage in the event of an audit for being non-compliant. If you don't know what those standard best practices are, contact your rep today and request documentation.

Remember, as with any type of insurance, just because you have it does not mean you're instantly covered for any and every type of incident. It's crucial to have an expert review your policy and identify the gaps in coverage.

Get Complete Security through DiamondIT



What's the first step in knowing where you are going?

Knowing where you already are.

Do you know if your network is completely secure? Do you have compromised credentials lurking in the Dark Web? Are you tempting malware hackers with a weak frontline? If you are not verifying your security on all levels, that uncertainty could be costing your employees valuable time and energy, while impacting your bottom line.

Let the team at DiamondIT conduct a vulnerability and risk management assessment to determine what tools you have in place to minimize the chance of a cyberattack. We can determine where your network may be most susceptible to intrusion. We can help document a process for restoring the business in the event of a catastrophe. We can even conduct a free Dark Web scan.

Contact us today at 877-716-8324 or online: www.diamondit.pro

FREE DARK WEB SCAN | **SECURITY ASSESSMENT** | **TECH CONSULTATION**

About DiamondIT

At DiamondIT, we understand your business is unique, and the tech solutions you need to run your business are equally unique. As we celebrated our 10th anniversary of helping our clients fulfill their missions with comprehensive and worry-free tech and IT solutions, we reflected on our own mission:

Mission Statement

By providing our people an outstanding work experience, our clients will consistently receive uncompromised quality and peace of mind.

Originally established in 1997 as a hardware reseller, Diamond Technologies, Inc. grew by capturing large computer hardware and software contracts throughout California. As the industry changed, Diamond Technologies re-invented itself in 2005 as an IT consulting, support and training organization specializing in all facets of business technology. In 2015, the company updated its marketing and branded as DiamondIT to reflect its standing as a premier technology consulting firm.

Today, DiamondIT is a strategic technology solutions provider that offers our clients a single point of contact for ALL their technology needs.

DIAMOND IT
your potential. our passion.