NAVIGATING THE CYBERSECURITY CRISIS

A CEO's Essential Guide to Safeguarding Your Business In the Digital Age

Provided as an educational service by:

Darren Crane, President
DLC Technology Solutions, Inc.
777 Route 70 E, Suite G-104, Marlton, NJ
856-983-2001 - dlctechnology.com
hello@dlctechnology.com

Are you wondering if you'll be the next victim in the cyber nightmare? You've heard the horror stories, now brace yourself for the reality...

Companies paralyzed as ransomware strikes like a thief in the night, bringing business to a screeching halt because of impatient and relentless demands for outrageous amounts of money.
Secrets exposed as thousands of sensitive client records are stolen and released on the dark web.
A financial bloodbath with hundreds of thousands—*even millions of dollars*—hemorrhaging from company coffers to make themselves whole again.
Brand and business reputations tarnished, and legacies forever tainted by exposed vulnerabilities.

And the haunting question you can't help but wonder…

"Am I truly safe and doing everything necessary to protect my business from the growing sophistication and threat of cybercriminals or am I just another lamb awaiting the cyber slaughter?"

If any of this rings true, this special report isn't just a wake-up call—*it's your lifeline*.

Ignore it at your peril.

Introducing…

Navigating the Cybersecurity Crisis: A CEO's Essential Guide to Safeguarding Your Business in the Digital Age.

Dear Fellow Business Owner,

First off, thank you and congratulations. Your decision to download this special report may be your most crucial move this year. Brace yourself for a stark revelation. This isn't just a report. It's your battle plan for survival in a world where cyber predators lurk in every corner. I aim to inform you of businesses' increasing cybersecurity threats and provide solutions.

At the end of this eye-opening report, you'll discover how to claim a free risk assessment valued at over $5,000 that could mean the difference between prosperity and digital disaster. Your free risk assessment analyzes external and internal cybersecurity threats. A report is produced with action items to mitigate the threats. Near the end of this special report, you'll find more information about how to obtain this free assessment, which will become your blueprint for fortifying your business against the rising cyber chaos.

In titling this report, I did not use "cybersecurity crisis" lightly. Make no mistake: "cybersecurity crisis" is an understatement. The evidence is undeniable. Cybersecurity threats pose a serious and growing risk to global stability, economic systems, and national security. The increasing frequency, sophistication, and impact of cyberattacks and the challenges in mounting effective defenses against invisible armies indicate that the world is, indeed, facing a cybersecurity crisis. The attacks are relentless. The stakes? Nothing short of everything you've worked your whole life to build.

My goal with this report is to give you more than information. It's the ammunition you need to mitigate your risk and repel the dark forces threatening to tear your business apart. With it, you can face the storm and lessen the chances that your business falls prey to a crippling attack.

Best regards,

Darren Crane
President, DLC Technology
856.983.2001

Navigating the Cybersecurity Crisis: A CEO's Essential Guide to Safeguarding Your Business in the Digital Age.

In today's rapidly evolving digital landscape, businesses face an unprecedented cybersecurity crisis. With cyberattacks increasing in frequency and sophistication, organizations of all sizes are vulnerable to potentially devastating breaches.

As a business leader, understanding and addressing these cyber threats is no longer optional—it's a critical component of your leadership role. This report offers vital insights and strategies to navigate the challenging realm of cybersecurity, safeguard your business assets, and uphold stakeholder trust in a hostile digital environment.

Table of Contents

Cyber Menace Unleashed: The Rising Tide of Nation-State Attacks

Nation-state-sponsored cyberattacks are growing at an alarming rate. The four main countries that sponsor these attacks are China, Russia, Iran, and North Korea. Some cybercriminals are employed by government agencies, working 9-to-5 hours in an office-like setting. Others result from these governments collaborating with organized crime groups and freelancers. This allows them to maintain plausible deniability when a cyberattack occurs. On top of nation-state-associated cybercriminals, freelancers are working around the clock, seeking to enrich themselves on your dime.

A driving motivation for these cybercriminals is financial gain, of course. However, for some, the goal is to steal sensitive information from corporations and governments. Others want to disable critical infrastructure or services, which was the case when Russian hackers attacked Ukraine's power grid. Some do it for political influence and to sow discord.

The big takeaway is that there are thousands of people around the globe working 24/7 whose only goal is to hack into your computer network and cause you harm. According to the 2023 Official Cybercrime Report by Cybersecurity Ventures, the annual global costs from cybercrime damage are expected to reach 10.5 trillion USD in 2025!

Here are some alarming statistics that reflect the growing frequency and sophistication of cyberattacks. Awareness of these statistics is ample motivation for your business to develop effective strategies to combat the ever-growing landscape of cyber threats.

- ✓ **Globally, there are, on average, 1,636 attacks per organization per week**, according to Check Point Research, with the three most attacked industries being Education/Research (3,341 attacks per week), Government/Military (2,084 attacks per week) and Healthcare (1,999 attacks per week).

- ✓ According to the IBM Cost of Data Breach Report 2024, **the average cost of a data breach globally was $4.88 million in 2024—a 10% increase over last year and the highest total ever**.

- ✓ In the fourth quarter of 2023, **the average ransom payment for cyber-attacks in the United States amounted to over 568,000 USD**, down from nearly 850,000 USD in the third quarter of 2023. This figure has increased significantly since the first quarter of 2022, when the average ransom payment amount in the US was approximately 212,000 USD, according to statista.com.

- ✓ Eighty-two percent of ransomware attacks in 2021 were against companies with fewer than 1000 employees, with **37% of ransomware victims being companies with fewer than 100 employees**, according to a report by Coveware.com.

Why are so many businesses with under 100 employees being targeted?

Cybercriminals are keenly aware that smaller businesses have fewer security protections than larger enterprises. Plus, attacks on small to medium-sized businesses are less likely to receive media and law enforcement attention than larger ones.

There's another reason. It's a strategy called "island hopping." Cybercriminals gain access to smaller companies and use them as a stepping stone to bigger companies with which the smaller company has a business relationship. By infiltrating a smaller company, a hacker can gain access to a larger company's network details, security protocols, and business relationships. Once they have the information they need to hack the larger company, they will instigate a ransomware attack against the smaller business.

So, if you think you are too small to be of any interest to the thousands upon thousands of hackers across the globe, you're not. While you might believe your client data is of no interest to them, you're mistaken. *Because it's valuable to you, it's valuable to them.*

The National Cyber Security Alliance reports that one in five small businesses were victims of cybercrime last year. That number is growing rapidly as cloud computing and mobile device use increases. This figure might even be low, as many small businesses are embarrassed to admit they were a cyberattack victim.

While there are lots of statistics online with varying numbers regarding the number of weekly threats and the average ransomware cost, the overall trend is that businesses worldwide are in a *cybersecurity crisis*, which will only worsen.

The Financial Fallout: Can Your Business Weather the Cyberstorm?

Experiencing a data breach or ransomware attack can be financially devastating for a business. The financial implications can be severe and multifaceted. The following are costs you can expect your business to incur:

- **The Ransomware Price Tag: Can You Afford the Risk?** — A 2020 report by Sophos found that ransomware attack remediation efforts (downtime, people time, device cost, network cost, lost opportunity, etc.), on average, cost $732,500 when a ransom is not paid and $1,448,458 when a ransom is paid.

- **Downtime Disaster: The Clock is Ticking!** — The average downtime for businesses hit with a ransom attack in the US as of the second quarter of 2022 was 24 days, according to statista.com. A survey by Infrascale found that 10% of small and medium-sized businesses' downtime costs exceed $50,000 per hour, and for the rest, it ranges from $10,000 to $40,000 per hour. According to IBM's 2021 Cost of a Data Breach report, the average organization took 286 days to identify and contain a breach.

- **Government Fines: Are You Prepared for the Financial Fallout?** — If you are found to have inadequate security practices that lead to a data breach, you could be fined under the Federal

Trade Commission (FTC) Act. If your business is in the financial sector and found to be not compliant with the Gramm-Leach-Bliley Act (GLBA), you could face a fine of up to $100,000 per violation. If you operate in the medical sector and are found non-compliant under the Health Insurance Portability and Accountability Act (HIPAA), finds range from $100 to $50,000 per violation, with a maximum of $1.5 million for all violations in a single calendar year. If you are found to be in non-compliance with the Cybersecurity Maturity Model Certification (CMMC), you could be disqualified from bidding on Department of Defense contracts. Plus, some states have their own data protection acts, which issue penalties.

- **Legal Fees: The Hidden Costs That Keep Adding Up!** — Legal fees are one of several significant costs your business faces after a data breach. You'll need to hire lawyers to navigate compliance requirements and breach notification laws, defend against lawsuits from affected customers or business partners, and deal with regulatory investigations.

- **Lawsuits Looming: Are You Next?** — You could be the target of a class action lawsuit (or lawsuits) after a data breach. For example, a Florida-based company called National Public Data faces at least eight lawsuits after a massive data breach on December 30th, 2023.

- **Unexpected Expenses: The True Cost of Recovery!** — Your business will be responsible for incident response and recovery costs. Plus, you will be on the hook to provide affected clients with credit monitoring services should they be required. Your cyber insurance premiums will increase.

- **Data Loss Devastation: Can Your Business Survive?** — According to the Global Security Research Report, 29% of data breaches lead to data loss. The consequences are more financial losses and operational disruption. According to a University of Texas study, 94% of companies that suffer a catastrophic data loss do not survive—43% never reopen, and 51% close within two years.

- **Reputation Ruined: Is Your Brand at Risk?** — If your business suffers a data breach, it will suffer negative publicity and a loss of customer trust, impacting sales and revenue. Your company might have trouble attracting top talent and securing future investments.

Understanding these potential costs is crucial for businesses to prepare and implement effective cybersecurity measures to mitigate the risks associated with data breaches and ransomware attacks.

Unmasking Cyber Nightmares: Your Ultimate Battle Plan Against Digital Threats

Prepare yourself for a harrowing journey into the cyber warfare that exists. What follows is not a list to skim over lightly, but a catalog of nightmares that could shatter your business at any moment. But fear not because for each abomination unleashed by the underworld's nefarious hackers, we offer you a shield, a sword, and a beacon of hope so you can survive and arm yourself against these threats.

- **Deceptive Shadows: Phishing and Social Engineering** — Through deceptive e-mails, messages, and websites, phishing attacks trick individuals into revealing sensitive information. Social engineering exploits human vulnerabilities rather than technical vulnerabilities. It is when cybercriminals manipulate, influence, and deceive people to gain control of their computer system or steal confidential information.

  Solution: Implement phishing-resistant multi-factor authentication (MFA) to secure accounts. Utilize integrated cloud e-mail security solutions to analyze and isolate suspicious e-mails. Educate employees through regular security awareness training and phishing simulations to recognize and report phishing attempts.

- **Digital Hostage Crisis: Ransomware and Malware** — Ransomware encrypts a victim's files or locks their system, rendering data inaccessible until a ransom is paid for the decryption key. The ransom demand often comes with a deadline, threatening to permanently block access or increase the ransom if not paid in time. Malware, short for "malicious software," is any software intentionally designed to cause harm to a computer, server, client, or network. The malware aims to gain unauthorized access to systems, disrupt operations, and steal sensitive information.

  Solution: Implement endpoint protection tools with specialized ransomware features like device rollback (reversing changes by restoring a backup taken before modifications were made). Establish data loss prevention measures such as regular backups and recovery plans. Utilize secure DNS (Domain Name System) web filtering solutions to restrict access to harmful sites.

- **The Vault Breakers: Data Breaches** — A data breach occurs when unauthorized individuals obtain access to confidential or protected information. This unauthorized access to confidential information leads to potential identity theft and financial loss.

  Solution: Encrypting sensitive data provides extra security against unauthorized access. Only essential personnel should be granted access to sensitive information, following the principle of least privilege (the principle of least privilege is an information security concept that maintains that a user or entity should only have access to the specific data, resources and applications needed to complete a required task). Regularly update software and systems to patch vulnerabilities.

- **Password Pitfalls: Weak Passwords and Poor Security Practices** — Weak passwords make it easier for cybercriminals to gain unauthorized access, leading to data breaches, data loss and complete system takeover.

  Solution: Mandate using strong passwords or passphrases that are difficult to guess. Use unique passwords for each account. Regularly change passwords. Limit unsuccessful logins.

Use MFA. Most importantly, a non-web browser password management program should be used to generate and store unique passwords for each account.

- **The Barrage: Denial-of-Service (DoS) Attacks** — A Denial-of-Service (DoS) attack is a cyberattack that aims to render a machine or network resource inaccessible to its intended users by disrupting the host's services. Typically, this is done by bombarding the targeted machine or resource with unnecessary requests to overwhelm systems and block legitimate requests. DoS attacks disrupt without stealing data.

  Solution: Implement firewalls and intrusion detection systems to filter out malicious traffic. Restrict the server's acceptance of requests to a specific number within a certain time interval. Use multiple servers and data centers to distribute traffic and reduce the impact on any single resource.

- **The Enemy Within: Insider Threats** — Businesses face a significant cybersecurity risk from insider threats, where individuals within the organization misuse their access to systems and data. These threats can be intentional or unintentional, leading to severe consequences for businesses. It could be someone, such as a disgruntled employee, with authorized access seeking to intentionally harm your business by selling confidential data or introducing malware into your network. They could also inflict harm by colluding with an external third party. Threats can also occur unintentionally as a result of employee error or carelessness.

  Solution: Organizations must adopt comprehensive strategies that include monitoring, access management, training, and incident response planning to mitigate these risks effectively. User activity should be monitored for suspicious behavior, and strict access controls should be implemented based on job roles. It's critical to conduct thorough background checks during the hiring process.

- **Infiltration via Allies: Supply Chain Attacks** — Supply chain attacks are sophisticated cyberattacks that target an organization by exploiting vulnerabilities in its supply chain, often through third-party vendors or service providers. These attacks leverage trusted relationships between organizations and suppliers and can cause widespread and devastating damage.

  Solution: Conduct thorough security assessments of third-party vendors before engaging with them. Implement contractual requirements for vendors to maintain robust cybersecurity practices. Perform regular audits of third-party vendors' security measures and practices. Limit the access that third-party vendors have to critical systems and data. Use network segmentation to isolate sensitive areas of the network from potential threats. Employ continuous monitoring solutions to detect abnormal behavior or unauthorized access attempts within the network. Use threat intelligence solutions to stay informed about emerging supply-chain-related threats. Educate employees about the risks associated with supply chain attacks and how to recognize potential threats.

By addressing these threats with the appropriate solutions, businesses can significantly enhance their cybersecurity posture and reduce the risk of falling victim to cybercriminal activities.

Beyond the Basics: Fortifying Your Defenses Against Evolving Cyber Threats

I've run into businesses that are under the mistaken belief that having anti-virus software installed is enough to protect them from a cyber-attack. This misconception can give businesses a false sense of security and leave them under the impression that they have all their cybersecurity requirements covered. The primary focus of anti-virus software is to detect and remove malware. It does not come close to addressing the full spectrum of threats businesses face today.

Besides anti-virus software, the following are what most in the industry consider basic cybersecurity measures: firewalls, regular updates and patch management, strong authentication, employee training, data encryption, regular backups, access control, incident response plans, vulnerability scanning, and intrusion detection systems.

Here's the thing: even the above basic measures are not enough because of the evolving nature of cyber threats. Cyber attackers continuously develop new tactics and exploit emerging vulnerabilities that basic measures may not address. Advanced persistent threats (APTs), where attackers gain access to your network and maintain a presence undetected over an extended period and zero-day exploits where attackers take advantage of software vulnerabilities, require defenses beyond the basics. As businesses adopt more complex IT environments (cloud services, remote work setups, and diverse devices), they face increased attack surfaces that demand more comprehensive security strategies.

So, while basic measures are essential, they must be supplemented with advanced security practices such as continuous monitoring, threat intelligence integration, and a Zero Trust security model to mitigate modern cybersecurity risks effectively.

Cyber Insurance Isn't Enough: Why You Need a Robust Defense Strategy

Sometimes, I get pushback from business owners, who tell me they feel their financial risk will be limited because they have cybersecurity insurance. They don't care about having a comprehensive cybersecurity strategy. While cyber insurance is an essential component of risk management, it should complement, not replace, a robust cybersecurity strategy. Here are some points to consider:

- Cyber insurance policies often have specific exclusions and limitations. They may not cover all types of cyber incidents, especially those caused by human error or insider threats. It's crucial to understand what is and isn't covered to avoid unexpected gaps in protection.

- Insurers conduct thorough risk assessments to determine a cyber incident's likelihood and potential impact. Businesses with resilient cybersecurity measures in place are less risky, which

can result in lower insurance premiums.

- A cyberattack can cause significant financial losses that exceed policy limits. Costs related to business interruption, reputational damage, and legal fees can quickly add up, highlighting the need for comprehensive security measures.

- Businesses across various industries must implement specific cybersecurity measures to meet regulatory requirements. Insurance does not fulfill these requirements; non-compliance can result in fines and penalties.

- As cyber threats evolve, insurance policies may struggle to keep up with the ever-changing risks. Businesses must regularly revise their security strategies to respond effectively to these changes, as insurance alone cannot meet the demand.

- Insurance policies do not shield individuals or businesses from legal responsibilities. If a company is non-compliant with cybersecurity regulations or has ineffective security practices, it can still face legal action, fines, and criminal charges. Plus, coverage can be denied if cybersecurity measures are not in place or being followed.

So, while insurance is designed to mitigate financial losses after an incident, it doesn't prevent breaches from occurring. Robust cybersecurity measures are needed to protect against attacks and protect you from additional costs because of fines and legal action against your business.

Zero Trust Security: The Ultimate Fortress for Your Digital World

Zero Trust Security is a cybersecurity framework that operates on the principle of "never trust, always verify." It requires strict identity and permission verification for **every user, device and application** attempting to access resources, regardless of their location within or outside the network perimeter.

In the case of Zero Trust on the endpoint computer, no longer does an application on your computer do whatever it wants! For example, there is no valid reason for Microsoft Word to be running a powershell script or to talk to another computer in a foreign country. A Zero-Trust environment will disable all actions by default unless specifically permitted. This helps shrink the attack surface, minimizes the impact of breaches, and offers strong protection against threats like ransomware and insider attacks as it cripples the processes ability proceed with the infection. Zero Trust Security proves particularly valuable for businesses with distributed remote workers, hybrid cloud environments, and any business where the cost of downtime is intolerable.

The Human Factor: Unmasking the Real Cybersecurity Culprit

Human error is the driving force behind all cybersecurity problems. A 2020 report by Stanford University researchers in conjunction with a top cybersecurity organization found that approximately 88% of all data breaches are caused by an employee mistake. The most common type of human error is when people fall victim to phishing scams and social engineering attacks, use weak passwords,

deliver sensitive data to the wrong e-mail recipient, and leave devices unsecured.

Cyber Savvy: Elevating Your Team with Dynamic Training

For training to accomplish its goals, upper management must be 100% on board. Your leadership team should actively participate in training programs to demonstrate commitment and set an example for the rest of the organization. For a comprehensive cybersecurity training program for businesses, it is essential to include various vital components that equip employees to tackle cyber threats effectively. These are the key components that cannot be overlooked:

- **Empowerment Through Employee Training** — Provide foundational knowledge on cybersecurity best practices, including recognizing different types of cyberattacks and understanding company policies. Ensure employees understand how to use safeguards such as anti-virus software, firewalls, and spam filters. You must provide regular updates and refresher courses to inform employees about new threats and security measures.

- **Feedback: The Catalyst for Continuous Improvement** — Feedback is an excellent way to determine whether the training was practical and met its goals. Feedback gives trainers the information they need to adjust the training to meet employee needs. Collecting and reacting to feedback will make future training sessions more relevant and engaging. It also boosts employee engagement in the training and motivates them to want to take part in future training sessions.

- **Stay Sharp with Ongoing Phishing and Social Engineering Awareness** — Develop and enforce comprehensive cybersecurity policies covering access control, incident response, and data protection. Establish clear procedures for reporting and responding to cyber incidents. Regularly test and update these plans to ensure effectiveness during actual attacks.

- **Fortify Your Defenses with Robust Policy Development** — Conduct phishing simulations and social engineering exercises to help employees effectively recognize and respond to these threats. Use quizzes and simulations to evaluate employees' understanding of cybersecurity concepts. Provide additional training for those who need it. Assign risk scores based on employee performance in assessments to identify areas needing improvement.

The above training components will enhance your organization's security posture by fostering a well-informed workforce capable of mitigating cyber risks.

Avoiding the Cybersecurity Trap: Choosing the Right IT Partner

When choosing an IT and cybersecurity partner, knowing the difference between a traditional IT company and an MSP is critical. A traditional IT company operates on the "break/fix" model. As a problem arises, they will provide the necessary services to fix it. They generally charge per hour or project. An MSP provides ongoing management and support to a company's IT infrastructure on a

subscription basis. They proactively manage and monitor systems to prevent issues before they occur, which minimizes downtime and ensures smooth business operations.

While IT companies recognize the importance of cybersecurity, not all handle it directly or effectively. Many IT companies outsource their IT needs to specialized firms (like MSPs). Many IT companies lack the budget, tools, and resources to offer comprehensive IT services. A shortage of qualified cybersecurity experts makes hiring and retaining top-quality talent difficult for some IT companies. It's imperative that you partner with an MSP with a high level of expertise in cybersecurity and who is continually investing in the latest cybersecurity innovations and technology. Note: At the end of this report is a quiz to determine if your current IT company is doing its job effectively.

Unlocking Cyber Resilience: The Independent Risk Assessment

Does your business have cybersecurity measures in place to protect your sensitive data and reduce your risk of being the victim of a data breach or a ransomware attack?

Having an independent third-party review your technology environment and cybersecurity stance on a regular (no less than annual) basis is a modern-day necessity. This allows your IT team to have an 'check and balance' against their day to day management of the environment and is a healthy way to ensure protections are working, modern and appropriate. **When was the last time an independent third-party reviewed your cybersecurity stance?**

If you have even the tiniest bit of doubt or want firsthand confirmation by a third-party firm then we need to have a conversation. ***When we speak I'll explain what our offer of a FREE cybersecurity assessment includes, and how your business can qualify. I'll also explain how this assessment is a truly independent, third-party view of your security through our use of an independent cyber partner.***

An independent risk assessment provides numerous benefits, including expert insights that leverage specialized knowledge and industry best practices to identify overlooked IT policy and configuration gaps. The evaluation also provides actionable recommendations for continuous improvement, enabling your business to adapt to new threats and maintain robust cybersecurity. By identifying vulnerabilities early, independent assessments help prevent costly breaches and reduce the financial impact of potential cyber incidents.

Three ways you should be engaging a third-party

Engaging an independent third-party can be a game-changer for ensuring your cybersecurity protections are up to par. One of the key services they offer is a **Risk Assessment**, where they thoroughly evaluate your current cybersecurity practices and identify areas of exposure. This process helps you understand the specific risks your organization faces, whether it's weak access controls,

outdated software, or other vulnerabilities. The result is a prioritized action plan, helping you address the most critical security gaps before they can be exploited.

Next, a **Vulnerability Scan** can provide a technical deep dive into your network. This scan uses automated tools to identify known vulnerabilities, misconfigurations, and security weaknesses across your systems. It's an essential part of maintaining up-to-date defenses, as it continuously checks for newly discovered threats or security holes that could put your data at risk. Monthly vulnerability scans ensure you're staying ahead of attackers looking to exploit these flaws.

For a more thorough test of your defenses, consider a **Penetration Test**. This service goes beyond scanning by simulating real-world cyberattacks to assess how well your security measures hold up against skilled hackers. A penetration test allows a security expert to try and breach your systems in the same way a cybercriminal would, exposing weaknesses that might not be caught by automated scans. The test results give you a detailed look at where your protections might fail in a live attack, providing actionable insights to strengthen your overall security posture. **Penetration Tests are often required by various compliances, and in general are recommended no less than once per year for all businesses.**

Together, these three services—Risk Assessments, Vulnerability Scans, and Penetration Tests—offer a comprehensive evaluation of your cybersecurity defenses. By working with a trusted third-party, you gain an objective view of your risks and the tools to safeguard your business from evolving threats.

My Offer To You: FREE Independent Risk Assessment

As my reward to you for reading this far into this whitepaper, I'd like to offer you a FREE, no obligation independent assessment of your cybersecurity status. Just one hour of your time via phone is all that is needed to take a significant step in strengthening the cyber health of your organization. A few days later we will deliver an assessment report allowing you to gauge where your cybersecurity is today and how to improve it tomorrow.

Here are a few issues covered in our FREE independent third-party risk assessment. The assessor will:

- **Check if your business's login credentials are on the Dark Web** — If your credentials are found, you can take immediate action before a data breach impacts operations.

- **Assess the robustness of IT systems against a range of cyber threats** — This will identify blind spots and vulnerabilities that some internal teams might overlook. It gives you a blueprint of what actions need to be taken immediately to prevent your system vulnerabilities from being exploited by cybercriminals.

- **Evaluate the resilience of backup systems against ransomware threats** — According to Sophos' report "The State of Ransomware 2023," the median recovery costs for victims using adequate backups are about half the cost incurred by those who paid the ransom. According to Veeam's 2023 global report called "Ransomware Trends," malicious actors targeted backups

in at least 93% of attacks in 2022. The period ransomware cybercriminals remain undetected in a business's systems (known as "dwell time"), gathering sensitive information, identifying vulnerabilities, and planning their attack strategy is around 43 days for small and medium-sized businesses, according to an article on wingswept.com. This means hackers might have already disabled the functionality of your backup—without your IT people knowing about it! Having reliable backups gives you a better chance of restoring your systems without incurring exorbitant ransomware costs.

- **Find out if your team is still using weak, reused, or easily crackable passwords** on your network. Determine if security best practices for managing passwords and credentials, including enforcing multi-factor authentication (MFA) for remote access, critical accounts, and admin access are employed.

- **Determine where sensitive data is stored** in your environment and if it is properly protected.

- **Test your network Perimeter Defense and firewall** configurations.

- Gauge where you cybersecurity is today, and sketch out **an action plan based on the vulnerabilities unearthed** — The action plan will transform assessment insights into practical measures, enhancing your ability to manage risks proactively.

To schedule your free independent risk assessment,

the first step is to go to https://dlctechnology.com/free-assessment

to book 15 minutes of my time. We can get to know each other a little better, I will answer any questions and provide you with the specifics of how the independent risk assessment is administered. If all parties are in agreement, we can also get the assessment on the calendar.

I want to be up front and say that not all businesses will qualify, and this offer is subject to quantity limitations, so act now before this offer expires!

If you prefer to contact me by e-mail or phone me right away, use the contact information below.

Dedicated to serving you,

Darren Crane
President, DLC Technology
E-mail: hello@dlctechnology.com
Direct: 856-552-3535

But Wait, I Had Another Thought:

When I talk to other IT professionals and CEOs who have been hacked or compromised, almost all told me they thought their IT guy "had things covered." I'm also very connected with other IT firms across the country to "talk shop" and can tell you most IT guys have never had to deal with the enormity and severity of attacks happening in the last few months. That's why it's VERY likely your IT guy does NOT have you "covered," and you need a preemptive, independent risk assessment like the one I'm offering in this report.

As a business owner, I understand that you must delegate and trust, at some level, that your employees and vendors are doing the right thing—but it never hurts to validate that they are. Remember, it's YOUR reputation, YOUR money, YOUR business that's on the line. THEIR mistake is YOUR nightmare. Are you willing to take the risk?

This makes me want to ask you: Is your current IT company doing its job? Is Your IT partner delivering optimal performance?

I've created this quick quiz to help you find out.

If your current IT company does not score a "Yes" on every point, they are NOT adequately protecting you. Don't let them convince you otherwise, and DO NOT give them a free pass on any of these critical points.

Further, it's crucial that you get verification on the items listed. Simply asking, "Do you have insurance to cover us if you make a mistake?" is good, but getting a copy of the policy or other verification is critical. When push comes to shove, they can deny they told you.

- ☐ **Have they met with you recently—in the last three months—to specifically review and discuss what they are doing NOW to protect you?** If you are outsourcing your IT support, they should, at a MINIMUM, provide you with an annual (preferably quarterly) review and report of what they've done—and are doing—to protect you AND to discuss new threats and areas you will need to address.

- ☐ **Have they told you about new and inexpensive tools such as Security Awareness Training for your company's credentials or advanced endpoint security to protect you from attacks that anti-virus cannot detect and prevent?** Tools like Security Awareness Training and advanced endpoint security can significantly enhance your company's cybersecurity posture.

- ☐ **Do they proactively monitor, patch and update your computer network's critical security settings daily? Weekly? At all? Are they reviewing your firewall's event logs for suspicious activity?** Verification should be provided to you and your team without you having to ask for it.

- ☐ **Have they EVER urged you to talk to your insurance company** to make sure you have the right kind of insurance to protect against fraud? Cyber liability? Did you involve them in your last

renewal?

- ☐ **Do THEY have adequate insurance to cover YOU if *they* make a mistake and your network is compromised?** Do you have a copy of THEIR CURRENT policy? Does it specifically cover YOU for losses and damages?

- ☐ **Have you been fully and frankly briefed on what to do if you get compromised?** Have they provided you with a response plan? If not, WHY?

- ☐ **Have they told you if they are outsourcing your support to a third-party organization? DO YOU KNOW WHO HAS ACCESS TO YOUR PERSONAL COMPUTER AND NETWORK?** If they are outsourcing, have they shown you what security controls they have in place to ensure a rogue technician living in another country would be prevented from using their free and full access to your network to do harm?

- ☐ **Do they have specially trained analysts and engineers on the latest cyber security threats and technologies rather than just winging it?** Do they have at least ONE person on their team with CISSP (Certified Information Systems Security Professional) or CISM (Certified Information Security Manager) certification? Do they have anyone on staff experienced in conducting security risk assessments?

- ☐ **Do they have a ransomware-proof backup system in place?** One of the reasons the WannaCry virus was so devastating was that it was designed to find, corrupt and lock BACKUP files. ASK THEM TO VERIFY THIS. You might *think* you have it because that's what your IT vendor is telling you.

- ☐ **Have they put in place a mobile device management solution and coached you on the creation of a WRITTEN policy for you and your employees?** Is the data encrypted on these devices? Do you have a remote "kill switch" that would wipe the data from a lost or stolen device, and is that data backed up so you CAN wipe the device and not lose files?

- ☐ **Do they have controls in place to force your employees to use strong passwords?** Do they require a monthly password update for all employees? If an employee is fired or quits, does the HR have a process to ensure ALL accounts are disabled and/or passwords are changed? Can you see it?

- ☐ **Have they talked to you about replacing your old anti-virus with advanced endpoint security that utilizes behavior analysis? Is it backed by a 24x7 Security Operations Center, or just the IT team's Help Desk?** There has been considerable talk in the IT industry that anti-virus is dead, unable to prevent the sophisticated attacks we see today.

- ☐ **Have they discussed and implemented "multi-factor authentication" to access highly sensitive data?** Multi-factor authentication is a necessity in today's cybersecurity environment.

- ☐ **Have they recommended or conducted a comprehensive risk assessment or penetration test every single year?** Many insurance policies require it to cover you in case of a breach. The law may require you to do this if you handle sensitive data such as medical records, credit card and financial information, social security numbers, etc.

- ☐ **Have they implemented web-filtering technology to prevent your employees from visiting infected websites or websites you DON'T want them accessing at work?**

- ☐ **Have they given you and your employees ANY kind of cyber security awareness training?** Have they offered to help you create an AUP (acceptable use policy)? Employees accidentally clicking on a phishing e-mail or downloading an infected file or malicious application is still the number one way cybercriminals hack into systems. FREQUENTLY training your employees is one of the most important protections you can implement.

- ☐ **Have they properly configured your e-mail system to prevent the sending/receiving of confidential or protected data?** Properly configured e-mail systems can automatically prevent e-mails containing specified data, like social security numbers, from being sent or received or can force them to auto-encrypt.

- ☐ **Are you still paying the same monthly fee as you did 24 months ago?** While this sounds a little silly - it can be a sign of outdated practices and protections, as costs are rising significantly each year.

- ☐ **Have they discussed new protections with you or told you about new protections being added to your environment in the past 24 months?** Cyber threats constantly evolve, and businesses must ensure that their security measures are current. Plus, many industries have specific compliance requirements that necessitate regular updates to security measures.

This questionnaire assesses whether your current IT company is taking comprehensive measures to protect your business from cyber-attacks. Its goal is to help you determine if your IT provider is effectively safeguarding your business against potential threats and providing you with a robust cybersecurity posture.

If you answered one or more questions, "no," we should have a conversation ASAP. You can contact me by e-mail or phone at hello@dlctechnology.com or 856-552-3535 or go to: https://dlctechnology.com/free-assessment to book your free 15-minute independent risk assessment consultation.