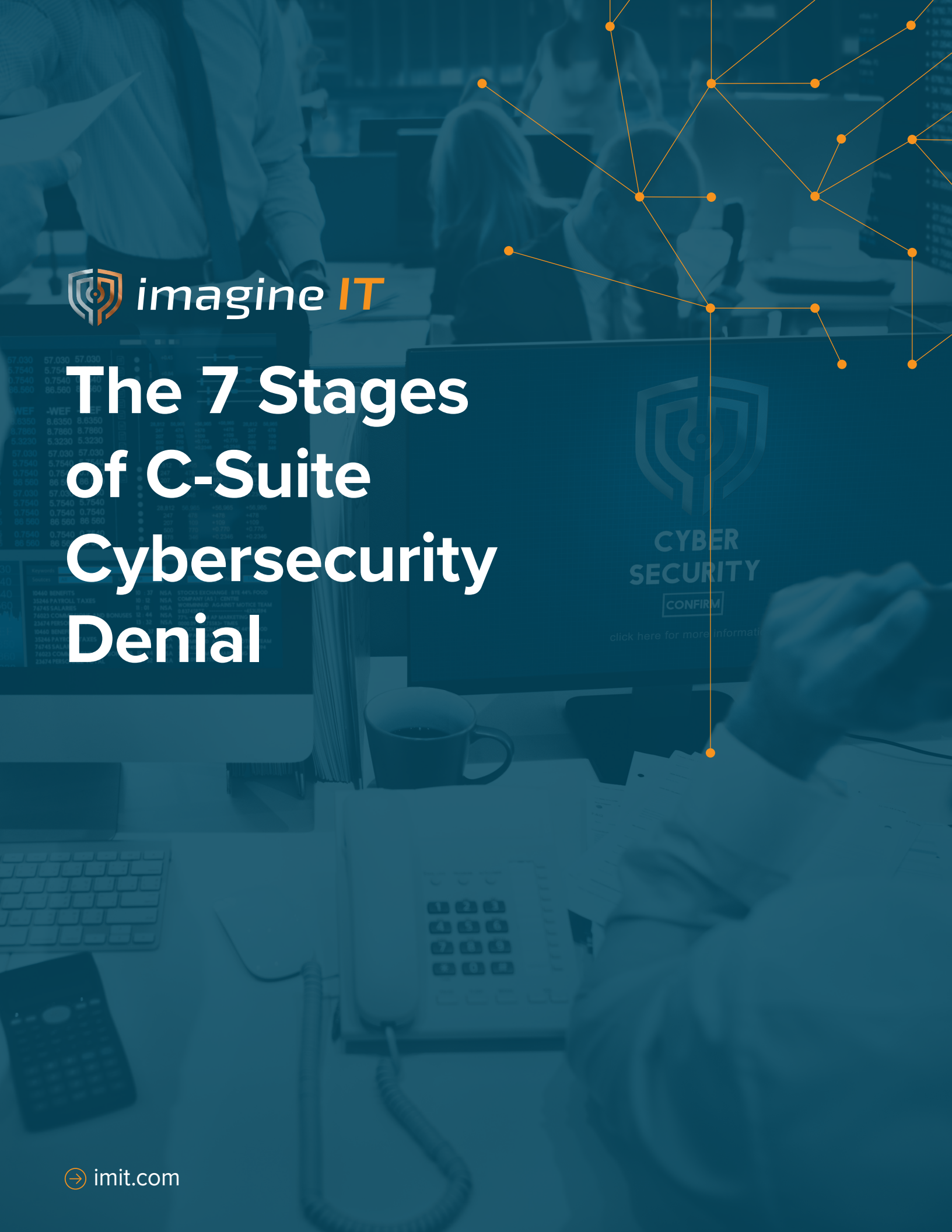


imagine IT

The 7 Stages of C-Suite Cybersecurity Denial

imit.com

The 7 Stages of C-Suite Cybersecurity Denial

The C-suite is responsible for managing risk, reputation, culture, and financial stability.

However, many executives incorrectly perceive cybersecurity as a "technical concern", not a "business imperative". Every year that assumption costs businesses billions of dollars and irreparable reputation harm. Executives do not need to define a tactical strategy, but they do need to manage risk and fully understand how the organization addresses it.

But before we get to the list, hear from a CFO that recently experienced many impacts of a serious cyber-attack:

60-Second Video...
http://ransomwarestory.imit.com/

As you just saw, that business was in denial and suffered the consequences, and this unfortunate outcome plays out hundreds of times per day. Is YOUR business in denial? Read on...

1. We are too small to be a target

It's a common misconception that small businesses are too insignificant to be targeted by cybercriminals. In reality, there are several reasons why smaller entities are often targeted.

Cybercrime can happen to anyone

- 75% of cyber-criminal victims are small orgs.
- Cyber-criminals attack businesses, nonprofits, churches, hospitals, schools, govt, public utilities – everyone.
- The perception (and reality) is that smaller orgs have weaker cybersecurity, and the cyber-criminals know this, increasing their chances of success.
- Many attacks are automated, regardless of victim org size.

Bottom line, you are not too small to be a target, you are just too small to make the news.

2. We have nothing a cyber-criminal would value

Small businesses hold several types of valuable assets that attract cybercriminals...

- Does your org have bank accounts? Credit card details, bank account numbers, and other financial data are highly lucrative for cybercriminals.
- Does your org maintain confidential information about staff or clients?
  - Personal details of employees, including Social Security numbers and payroll information, can be exploited for identity theft or fraudulent activities.
  - Client information such as names, addresses, phone numbers, and email addresses can be sold on the dark web or used for identity theft. Much of this type of data is regulated, leaving your org exposed to ransom and fines.
- Does your org hold intellectual property? Proprietary information, trade secrets, and business plans can be stolen and sold to competitors or used to gain a competitive advantage.
- Does your org work with larger companies? Small businesses often work with larger companies, and compromising a small business can serve as a gateway to attack bigger targets.

It's essential for small businesses to implement strong cybersecurity measures to protect these valuable assets.

3. The outcome won't be that bad

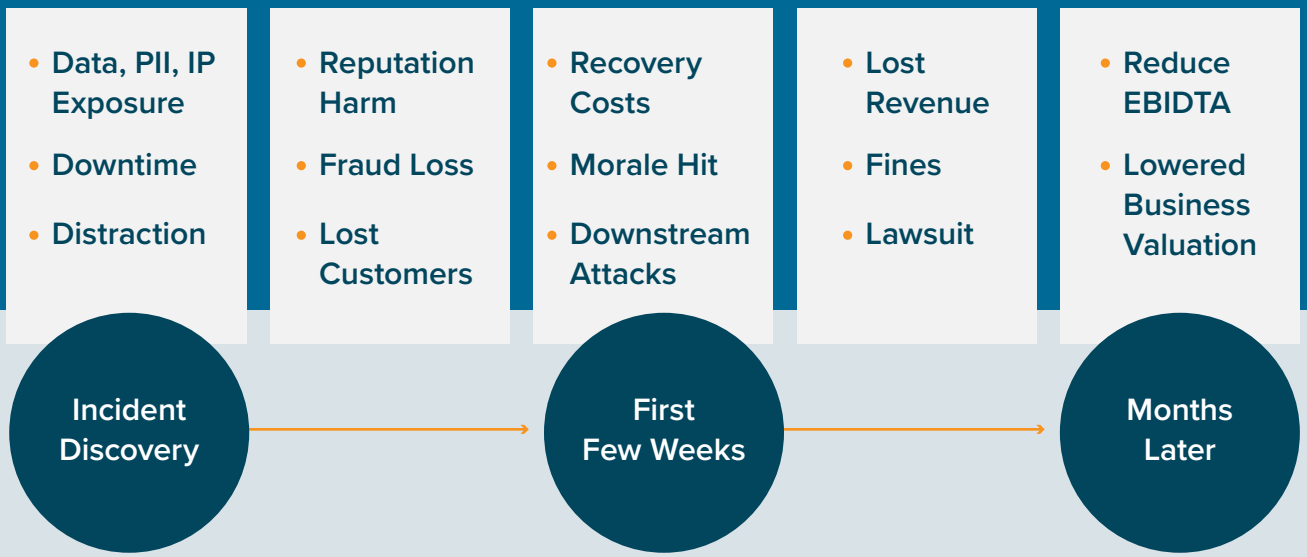
If you did not yet watch this 60-Second Video, please do so as the consequences to your org will surely be worse than you think... **http://ransomwarestory.imit.com/**

That video provides a glimpse into the devastating consequences of denial. In 2023:

- Cyber-criminals were able to destroy the backups in 70% of successful ransomware attacks, causing significant operational downtime and forcing a ransom payment.
- The average SMB ransomware claim was $345,000.
- The average social engineering finance fraud claim was $88,000.

Depending upon your industry, during a serious incident your org will suffer many of the consequences listed below...

Cyber Incident Impact Chain



4. Cyber insurance takes care of this

Proper cyber insurance coverage is crucial to business continuity and cash flow during an incident. But cyber insurance does not cover every type of attack, and carriers often limit reimbursements for certain types of attacks.

For example, carriers will not cover claims when:

- There were misleading or incorrect answers when completing insurance applications.
- There was prior knowledge of a vulnerability that was never addressed.
- It was determined to be a nation-state attack, as that is considered an act of war, even if the attack was for financial gain.

And how is cyber insurance going to reimburse reputational harm, and permanent exposure of confidential information or intellectual property?

You need to review your policy with a cyber insurance subject matter expert for gaps and limits.

Consider engaging with our CISO as he reviews multiple cyber insurance applications and coverage limits each week across our client base (see bottom of article for contact info). Even with proper coverage, no business ever wants to be forced to file a claim; it is best to avoid breach incidents in the first place.

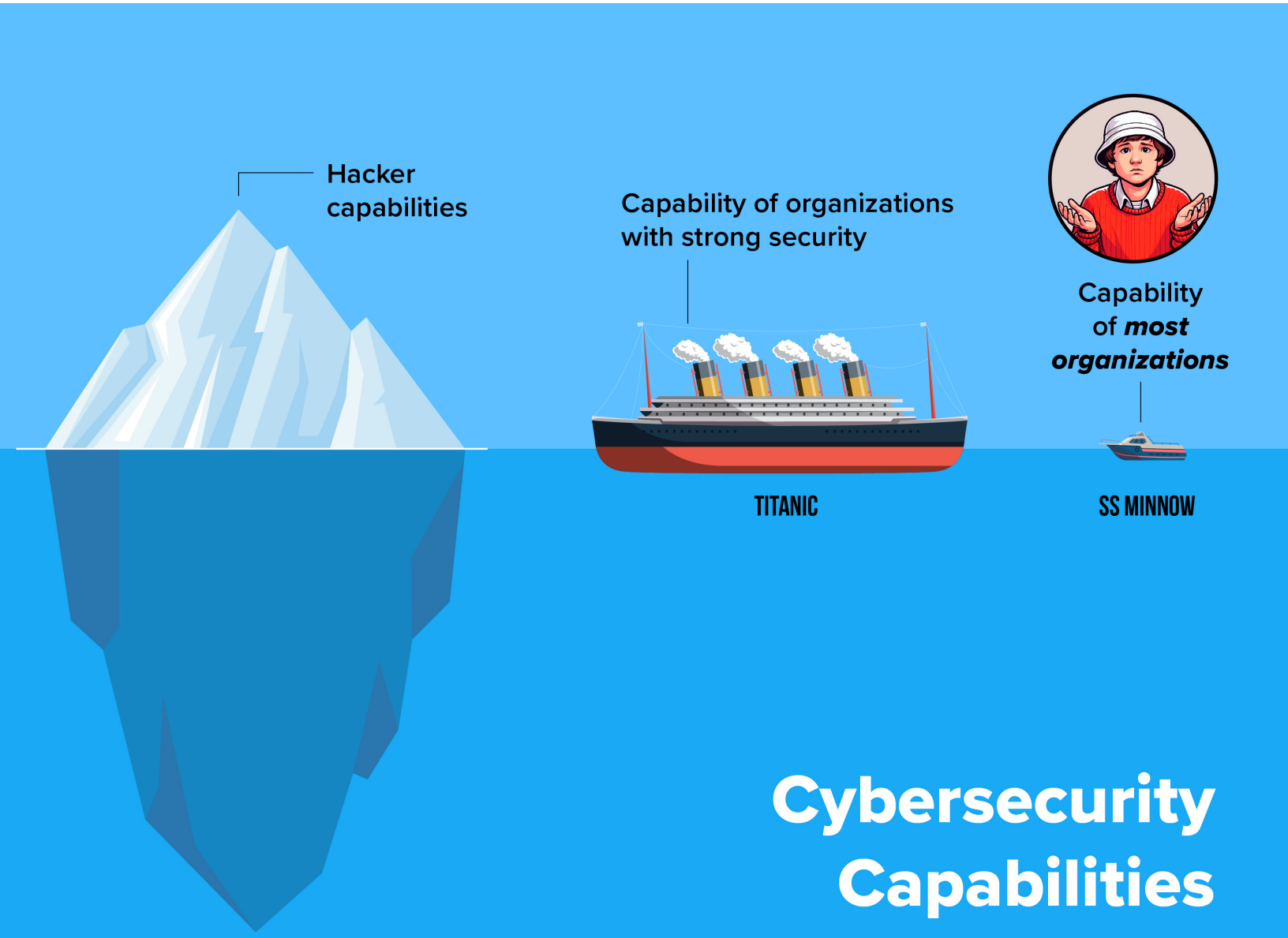
5. We can’t afford strong cybersecurity

A strong cybersecurity strategy is not an expense. It is an investment that protects your mission, your reputation, your profits, your valuation... ALL ROI.

Can you afford NOT to invest in cybersecurity? The financial consequences of a serious incident are severe.

You don’t need Fort Knox-level security, but you must implement robust cybersecurity measures that align with your organization’s needs. In my research, for as little as $15/user/mo you can make a huge improvement towards protecting your mission.

Bottom line, hackers choose to go after whatever is easy, and can get frustrated by orgs with strong security and will move on to easier targets. Don’t be the low hanging fruit...



6. Cybersecurity is a technical concern, not a business imperative

When viewing cybersecurity purely as a technical concern, decisions are made that do not align with the protection of the business mission; they are tactical and not strategic.

Cybersecurity has evolved into a critical “business imperative” for several reasons:

- Reputation and Trust: A data breach can severely damage a company’s reputation and erode customer trust. Maintaining robust cybersecurity measures helps protect the brand and build confidence among customers.
- Regulatory Compliance: Businesses must comply with various regulations and standards related to data protection and privacy. Failure to do so can result in hefty fines and legal consequences.
- Operational Resilience: Cyberattacks can disrupt business operations, leading to financial losses and downtime. Effective cybersecurity ensures operational continuity and resilience.
- Financial Impact: The financial repercussions of a cyberattack can be substantial, including costs related to remediation, legal fees, and potential loss of revenue.
- Competitive Advantage: Companies that prioritize cybersecurity can differentiate themselves from competitors by demonstrating a commitment to protecting customer data and maintaining secure operations.
- Risk Management: Cybersecurity is an integral part of overall risk management. By proactively addressing cyber threats, businesses can mitigate risks and safeguard their assets.

By viewing cybersecurity as a strategic business imperative rather than just a technical concern, orgs can better protect their assets and position themselves for long-term success.

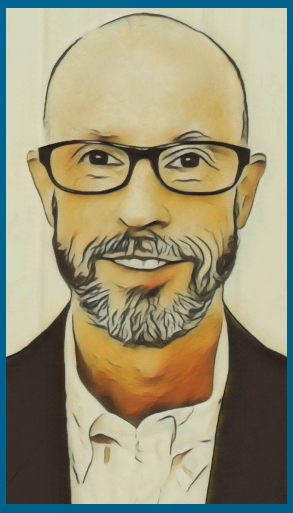
7. Our IT people have us covered

This is one of the most critical stages of denial. Protecting your data and mission is just too important to leave it entirely to IT people, even ones you trust.

Assuming your IT team has all aspects of cybersecurity covered is a critical mistake for several reasons:

- Specialization: Cybersecurity is a specialized field that requires specific skills and knowledge. While IT professionals are skilled in managing and maintaining IT infrastructure, they may not have the expertise needed to handle complex cybersecurity threats.
- Resource Constraints: IT teams often have multiple responsibilities, including network management, software updates, and user support. This can limit the time and resources they can dedicate to cybersecurity.
- Evolving Threat Landscape: Cyber threats are constantly evolving, with new vulnerabilities and attack methods emerging regularly. Keeping up with these changes requires continuous learning and adaptation, which can be challenging for a general IT team.
- Insider Threats: Not all cybersecurity threats come from external sources. Insider threats, whether intentional or accidental, can pose significant risks. IT teams may not always have the tools or processes in place to detect and mitigate these threats.
- Lack of Comprehensive Strategy: Effective cybersecurity requires a comprehensive strategy that includes risk assessment, incident response planning, and regular security audits. IT teams may not have the bandwidth to develop and implement such a strategy.
- Compliance Requirements: Many industries have specific regulatory requirements for data protection and cybersecurity. Ensuring compliance with these regulations often requires specialized knowledge and dedicated resources.

Partnering with external cybersecurity and compliance experts is essential for comprehensive protection.



Next Step – Take Action!

You now understand why cybersecurity is essential for your business. However, since you are not a cybersecurity expert, how will you find out where your business stands?

I would like to arm you with the “5 Critical Questions Executives MUST Ask IT Leadership”. Once you obtain the answers you will be able to start the process of reducing risk and protecting the mission.

If you would like access to the “5 Critical Questions…” article, discuss cyber insurance, or would just like more general guidance, please engage for a free 1-hr Business Cyber-Risk Consultation with our Founder, CISO, and cybersecurity thought leader, Peter Durand.

Click this link to *book a meeting* or type **peterd.imit.com** into your browser.