PROTECTING YOUR BUSINESS

Cyber Security & Cyber Insurance

A Comprehensive Guide for Modern Business Technology Challenges

Conscious.net

CONSCIOUS NETWORKS

In the digital age, where technology seamlessly intertwines with every aspect of business operations, the importance of cybersecurity cannot be overstated.

7 minutes. That's all it takes for an adversary to break in and move laterally to wreak havoc on your business. As your organization expands to new technology domains, it is critical to have the capabilities to secure them with a unified security solution that stops breaches across all key attack surfaces.

From small startups to multinational corporations, organizations of all sizes face an escalating threat landscape in the form of cyber attacks. The increasing sophistication of malicious actors poses a substantial risk to sensitive data, financial assets, and the overall stability of businesses. As businesses embrace digital transformation, the reliance on interconnected networks and online platforms makes them vulnerable targets for cybercriminals. Thus, prioritizing cybersecurity is not merely a choice but an imperative for safeguarding the integrity, confidentiality, and availability of critical information. Regardless of size, every business must recognize cybersecurity as an integral component of its strategic framework to ensure sustained growth, protect customer trust, and fortify its resilience against the ever-evolving landscape of cyber threats.

Table of Content

DRAFT - TO BE FINALIZED

43% of cyber attacks target small business.

75% of cyber attacks start with an email.

Human error accounts for 95% of all data breaches.

2023 Source: https://www.dbxuk.com/statistics/cyber-security

Understanding Cyber as a Business Culture

Today, Cyber is no longer a necessary evil - many businesses are adopting a mature approach to cyber by incorporating it into their business culture.

Understanding the Threat Landscape

In the fast-evolving landscape of technology, businesses and enterprises face an increasing array of cyber threats that can compromise sensitive data, disrupt operations, and damage the business' reputation. It's crucial to comprehend the evolving nature of cyber threats. Cybercriminals employ sophisticated techniques such as ransomware, phishing, and zero-day exploits to exploit vulnerabilities in business networks. As technology advances, so do the strategies of malicious actors. This necessitates a proactive and dynamic approach to cybersecurity.

The pandemic impacted the landscape significantly by making remote and hybrid teams commonplace. These work environments create millions more access points for hackers and bad actors to exploit businesses across the global landcape. Stopping data breaches requires timely understanding of the adversies, their methods, and their goals in order to protect your business properly.

The adoption of cloud based systems has further exacerbated the threat and the false sense of security. Many organizations expect their cloud providers to have proper protocols and systems in place. However, these organizations are also at the top of the food chain for exploitation. This particular area is critical to evaluate since it's not if, but when, a cloud provider is compromised, and what your organization will do to maintain your daily business operations along with responsive measures.

Every Second Counts

There is an entire underground network of adversaries that are not only trying to compromise business environments, but then in turn, provide or sell this access to other actors, including ransomware operators. According to Crowdstrike,

> There was a 71% increase in adversary tactics using valid credentials to access environments.

there was a 112% increase in 2022 compared to 2021 of brokered access techniques.

Malware has always been a challenge, but there was a 71% increase in adversary tactics using valid credentials to access environments. The technology, financial, and healthcare industries topped the list. However, public and private sectors are impacted along with small to medium sized businesses.

In each of these scenarios, when an attack occurs, every second counts. It's important to have a rigid prevention, detection, and recovery plan in place.

Cloud Consciousness

Utilizing the cloud has created a complex threat level that must be addressed by cloud providers as well as the businesses utilizing those services. In these cases, bad actors don't just steal data - they remove access to accounts, terminate services,

destroy data and delete resources. These actions can dramatically impact the daily operations of any business. For these reasons, it's important for businesses to have an individualized cyberstrategy outside the cloud, that layers on top of the cloud providers strategies. Backup and recovery strategies are essential while endpoint security and MDR are also vital services to consider, at a minimum.

Cyber is No Longer an IT Thing

According to the Deloitte 2023 Global Future of Cyber Survey, "Organizations increasingly recognize the role cyber plays in enabling broad business success." In the same report, Allan Cockriel, CIO of Shell, notes "We're doing a lot in terms of embedding cyber - whether its' DevOps or product development - where we're starting to co-create with partners to make sure that we are building things securely. It's like culture transformation."

it's important for businesses to have an individualized cyberstrategy, outside the cloud.

Many Boards recognize the shift too. Boards are discussing and evaluating the leaders and culture within their organizations and the impact of a mature approach to cyber culture and initiatives, at all levels. Instead of focusing on cyber as a necessary evil, these organizations are embedding information security, privacy, and business objectives into their processes and strategic planning. After all, a successful business model plans for moving the business forward in a compliant and secure manner.

A mature cyber conscious organization will incorporate cyber considerations in every aspect of their strategic plan. This may include requiring partners and suppliers to have certain protocols in place too. Cyber hygiene standards may be implemented for any new product or technology considerations or perhaps going beyond compliance requirements to create forward-thinking, secure and safe environments, for customers. These initiatives can impact operational stability, brand reputation and consumer confidence levels.

Where to Begin

Historically, cyber security has been an IT responsibility but cyber maturity requires enterprisewide engagement. The CIO, CISO, CFO, COO and General Counsel all have extremely valuable input and perspective.. For example, the CIO may be focused on technology and threats while the CFO may be focused on costs and operational efficiencies. Conversely, the COO or General Counsel may be focused on compliance and privacy challenges.

We believe the best scenario utilizes a holistic approach and the expertise of a trusted technology and business adviser. Ideally, this partner would have the resources and expertise to integrate each stakeholder's input along with overall business objectives. This is not an easy task, but Conscious Networks believes it is well worth the effort.

There is A Shift

As you can see, cyber is not just about threats. There is a dyanmic shift in business culture when it comes to the cyber landscape.

At Conscious Networks, we have been serving the C-suite and supporting IT teams for over 20 years. Our technology experitse, businesss acumen, and cyber security platforms are state of the art. But, more importantly, we serve to engage your business and leadership teams in a deeper and more meaningful way. This approach can help you adopt and foster a cyber mature culture so that you can move from an 'all hands on deck' approach to a more strategic, methodical and efficient businses model that protects your business while fostering growth. Isn't that a better way to move forward and plan for the future?

Every business
can benefit from
understanding that
Cyber is no longer just
an IT thing - it's culture
transformation.

Cyber Basics

FAQs and what the most basic cyber strategies include.

Building A Strategy

Implementing a robust cybersecurity foundation is imperative for any business, regardless of its size. At its core, basic cybersecurity measures involve the implementation of strong access controls and user authentication mechanisms. This includes enforcing complex passwords, utilizing multi-factor

authentication, and regularly updating credentials. Regular software updates and patches are essential to address vulnerabilities in operating systems and applications, thereby minimizing the risk of exploitation by cyber threats. Firewalls and antivirus software serve as fundamental defenses, safeguarding against unauthorized access and detecting and neutralizing potential malware threats. Furthermore, employee awareness and training programs play a pivotal role, educating staff on cybersecurity best practices, social engineering tactics, and the importance of responsible online behavior. Establishing a data backup and recovery plan ensures that critical information can be restored, in the event of a cyber incident. By adhering to these basic cybersecurity requirements, businesses can significantly enhance their resilience against common cyber threats and create a more secure digital environment.

What is Cybersecurity?
Cybersecurity is a broad term that can mean different things for different businesses and industries. In it's essence, it includes a comprehensive evaluation of your technology and processes in an effort to protect your business operations, networks, programs, all electronic devices (laptops, phones, tablets, etc.), and most importantly, your data, from cyber-attacks.

What is a Cyber-Attack?
A cyber-attack is when an entity infiltrates your network to disrupt operations, steal data, capture sensitive information, or tap into your intellectual property. Every business, regardless of their size, is vulnerable to cyber-attacks. Many small to medium sized businesses are the most viable targets because they do not tend to invest in the same infrastructure or prevention tools as a large enterprise. However, Conscious Networks advocates for the implementation of enterprise level solutions for small-medium sized businesses to prevent and discourage cyber-attacks.

What does a basic cybersecurity plan include?
While there is no 'one size fits all' cybersecurity plan, there are some key elements that will be implemented in virtually every strategy. These can include:

- Managed Detection and Response (MDR) systems,
- Endpoint security,
- Backup and recovery strategies,
- Managed services including antivirus, patch, and updates,
- Networking monitoring,
- Infrastructure analysis,
- Employee training

By incorporating these key considerations into your cybersecurity strategy, your business can enhance its preparedness against the evolving landscape of cyber threats, mitigating potential risks and ensuring the resilience of your digital infrastructure. This approach can also qualify you for discounts on your cyber insurance policy.

What is Social Engineering?
Social engineering in cybersecurity refers to the manipulation of individuals to gain unauthorized access to sensitive information, networks, or systems. Unlike traditional hacking methods that exploit vulnerabilities in software, social engineering relies on exploiting human psychology and trust. [See the Case Study on p. 12] Attackers use various techniques, such as phishing emails, impersonation, pretexting, or baiting, to deceive individuals into revealing confidential information, clicking on malicious links, or performing actions that compromise security. Social engineering attacks often prey on human emotions, curiosity, or urgency, making individuals unwittingly assist cybercriminals in their illicit activities. It underscores the importance of not only technological safeguards but also user awareness and education to recognize and resist such deceptive tactics. Employee training, across

your organization, is paramount to protecting your business from social engineering threats.

Cybersecurity Monitoring
Companies without a formal cybersecurity plan and infrastructure can take an average of 200 days to detect a cyber-attack. Routine check-ups and a cybersecurity plan help to ensure network safety through frequent updates, patches, and network monitoring. This service is often outsourced for 24/7 monitoring and detection.

Cyber In The Cloud
According to the latest data, it is estimated that 94% of busineses store data in the cloud. Many businesses, especially small businesses, rely on their cloud providers to protect their data and prevent cyber attacks; however, this is a big mistake.

The cloud is a primary target for attacks - hackers can create mayhem while holding confidential data hostage. Cloud providers have provisions for how they will respond to, and restore data, if/when a cyber attack occurs. However, what will your business do if you are without access to your data or systems for an extended period of time? There are many important considerations, but businesses must consider:

1. Utlizing a hybrid of public and private cloud services.
2. Ensuring you have a solid backup and recovery strategy, separate from what your cloud provider has in place.

Cyber-Attacks on Small-Medium Sized Businesses
A significant percentage of small businesses (64%) experience cyber-attacks annually. These cyber-attacks collectively cost businesses an estimated $400 billion yearly, with small businesses alone facing an average cost of $38,000 per year. If ranswomware is employed as part of the attack, the costs could rise significantly. This is why it's important for businesses of all sizes to have a cyber security plan and cyber insurance.

For small businesses, implementing robust cybersecurity measures is crucial to prevent cyber attacks and safeguard sensitive information. Firstly, ensuring the use of strong, unique passwords and

64% of small businesses experience cyber attacks annually.

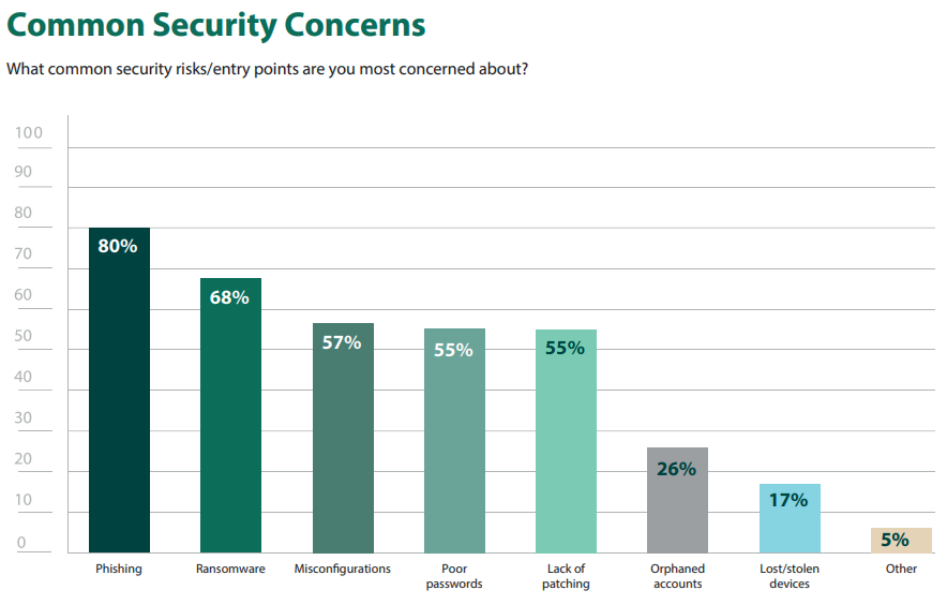
enforcing multi-factor authentication can significantly enhance account security. Regularly updating and patching software, including antivirus programs,

helps address vulnerabilities and protect against known exploits. Employee training plays a pivotal role; educating staff about the dangers of phishing emails, social engineering tactics, and the importance of maintaining a security-conscious mindset can prevent inadvertent security breaches. Additionally, restricting access to sensitive data on a need-to-know basis minimizes the potential impact of a security compromise. Backing up critical data regularly and storing it securely off-site provides a means of recovery in case of ransomware attacks. Employing a firewall and encrypting sensitive information also adds layers of defense against unauthorized access. Collaborating with cybersecurity professionals or leveraging managed security services can be beneficial for small businesses lacking in-house expertise. A comprehensive and proactive approach to cybersecurity significantly reduces the risk of cyber attacks for small businesses.

If you are a small-medium sized business, you may be asking what steps you can take to protect your business, in a methodical way, without breaking the bank. Fortunately, there are several ways to accomplish this. We often advise clients to start with best practices like these:

1. **Assessment** - The first step is to seek out a trusted technology partner, like Conscious Networks, to evaluate your current technology environment and infrastructure. By conducting a risk assessment, you will get a better understanding of your immediate and long term risks. This will also help you establish a budget for your initiatives. We strongly recommend having an outsourced technology advisor conduct the assessment. This will also help ensure that, if you have an internal IT department, they are following protocols and best practices.
2. **Start with the Basics -** Most SMEs start with detection and prevention strategies, a backup and recovery plan, and employee training, at a basic level. These types of services can be provided in conjunction with a 1, 3, or 5 year strategic plan. Every organization can enable some type of protection with basic monitoring and detection or MDR. If you have a large number of employees working virtually or in the field, endpoint security will also be key. Developing a solid backup and recovery strategy ensures that, in the event of a crisis, you're not starting from scratch. As time and business evolve, you can add additional layers of protection. Employee training is not expensive but is a critical component to consider on a regular basis.
3. **Budget vs. Risk** - Just like when you purchase E&O or Liability insurances, you have considerable options when it comes to cyber insurance. The key, we believe, is to balance your risk when considering insurance options.

Conscious Networks provides the guidance and technology to help you create a cybersecurity strategy for your business, regardless of your size or budget.



Source: https://terranovasecurity.com/blog/cyber-security-statistics/

A Case Study Worth Studying

When cyber attacks do occur, it can take days or weeks to get a businness' data secured and back online. Remember the 2023 debaucle of the MGM cyber attacks? Operations were brought to a halt and it was reported that **the business suffered an estimated $8.4 million dollars per day in revenue loss.**

In addition, countless lawsuits were filed by customers concerned about the security of their information and financial records. What a stark reminder that no organization is immune to cyber-attacks. This particular breach highlights several key lessons:

1. **Social Engineering Attack** - In this example, a hacker used Linkedin to identify a current employee, assumed their identify, and called the MGM IT help desk requesting assistance logging into their accounts. This tactic is where your business can be most vulnerable because it relies on human error, rather than vulnerabilities in software and systems. Ongoing employee training, processes, and awareness is paramount to reducing these types of risks.
2. **Monitoring & Crisis Plan** - Even though MGM detected unusual activity and deactivated servers and infrastructure, the hackers claimed to have already exfiltrated important client and business data, so every second counts. Does your internal IT staff have a crisis plan? Will your technology provider know what to do quickly to minimize your losses?
3. **Branding & Trust Factors** - The impact on the MGM brand is obviou. In this case, multiple class action lawsuits were filed which could result in millions of dollars. No doubt, many future customers now have a negative reference and perhaps, question the credibility of the brand. What happens to your business if you have to notify your customers that there has been a breach? Customer confidence is an important part of your brand. You are expected to protect personal and private information.
4. **Backup & Recovery Strategies** - While it is not exactly clear what MGM's backup and recovery strategy was at the time of the incident, we know that their operations were down for at least ten days. A solid backup and recovery plan may have allowed them to resume limited operations, with off-site services, equipment, and restored data. Colocation, cloud data management, offsite servers, and private cloud services may have also been helpful.

Zero Day Exploits

In the fast-paced realm of technology, where innovation is constant, businesses leverage cutting-edge solutions to stay competitive. However, with this progress also comes risk, and one of the most potent threats facing businesses today is the zero-day exploit.

Zero-day exploits pose significant threats to business technology, with far-reaching implications that can impact an organization's operations, data security, and reputation.

What is a Zero-Day Exploit?
A zero-day exploit refers to a cyber attack that takes advantage of a security vulnerability on the same day it is discovered or exploited. The term "zero-day" implies that the affected software vendor has zero days to address and patch the vulnerability before it is exploited by malicious actors. These exploits target undisclosed or unknown vulnerabilities, making them particularly dangerous.

The Element of Surprise
What makes zero-day exploits so nefarious is the element of surprise. Unlike known vulnerabilities for which patches may already be available, zero-day vulnerabilities are often unknown to both software vendors and the organizations using their products. Cybercriminals capitalize on this lack of awareness to launch targeted attacks before any defensive measures can be taken.

Targeting Specific Software
Zero-day exploits can target a wide range of software, including operating systems, web browsers, and even applications widely used in business environments. Attackers may employ various methods, such as phishing campaigns or drive-by downloads, to deliver malware that exploits the undisclosed vulnerabilities.

Data Breaches
One of the primary goals of zero-day exploits is unauthorized access to sensitive data. Whether it's customer information, intellectual property, or proprietary business data, a successful zero-day attack can lead to a data breach. The consequences of a data breach extend beyond financial losses, encompassing damage to reputation and customer trust.

Disruption of Operations
Zero-day exploits can disrupt critical business operations by exploiting vulnerabilities in essential software or infrastructure. This disruption can lead to downtime, affecting productivity and potentially causing financial losses. In sectors where uptime is paramount, such as finance or healthcare, the impact can be particularly severe.

Corporate Espionage
Zero-day exploits are often favored by cybercriminals engaging in corporate espionage. By infiltrating a business's systems and gaining unauthorized

access to proprietary information, competitors or malicious actors can gain a significant advantage. This can lead to a loss of intellectual property, trade secrets, and a decline in market competitiveness.

Financial Consequences
The financial consequences of a zero-day exploit can be staggering. Beyond the immediate costs of mitigating the attack and potential legal ramifications, businesses may also face regulatory fines for failing to adequately protect sensitive information. Additionally, the long-term impact on revenue and customer trust can be substantial.

Defending Against Zero-Day Exploits
Given the elusive nature of zero-day exploits, defending against them requires a multi-faceted and proactive cybersecurity strategy. Most mid-sized businesses consider outsourcing this element of their operations to a trusted technology provider whose core competencies are focused on identifying and remedying these exploits. Conscious Networks utilizes a holistic approach to technology to recommend the best options, given your business environment, compliance requirements, and risk profile.

- **Regular Software Updates** - While zero-day exploits exploit unknown vulnerabilities, organizations can minimize the risk by staying vigilant about software updates. Regularly updating operating systems, applications, and security software ensures that known vulnerabilities are patched promptly, reducing the attack surface for potential exploits.
- **Network Segmentation** - Implementing network segmentation is crucial for containing the impact of a zero-day exploit. By dividing the network into segments, organizations can prevent lateral movement by attackers, limiting their ability to traverse the entire infrastructure even if a breach occurs.
- **Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)** - Deploying IDS and IPS solutions can help organizations detect and prevent zero-day exploits. These systems monitor network and system activities for unusual patterns or behaviors that may indicate a potential attack. When anomalies are detected, these systems can take proactive measures to prevent the exploit from succeeding.
- **User Training and Awareness** - Human error remains a significant factor in cybersecurity breaches. Educating employees about phishing tactics, safe online practices, and the importance of reporting suspicious activities can significantly reduce the likelihood of successful zero-day attacks initiated through social engineering.
- **Threat Intelligence** - Utilizing threat intelligence services can provide organizations with early warnings about potential zero-day vulnerabilities. By staying informed about emerging threats and vulnerabilities, businesses can proactively implement defensive measures before malicious actors can exploit them.

In the ever-evolving landscape of cybersecurity threats, zero-day exploits stand out as particularly challenging adversaries. Their ability to strike with little warning and exploit unknown vulnerabilities makes them a formidable threat to business technology. Organizations must adopt a proactive cybersecurity stance, combining regular software updates, network segmentation, advanced detection systems, user training, and threat intelligence to effectively defend against the potential fallout of zero-day exploits. By understanding the nature of these threats and implementing comprehensive security measures, businesses can fortify their defenses and navigate the digital landscape with greater resilience.

It's not a question of
IF
your business will
experience a cyber
attack, but how well
prepared you are
WHEN
it happens.

Cyber Insurance

Common Questions & Answers

The purpose of cyber insurance is to provide financial protection in the event of a cyber-related incident or data breach. Cyber insurance, also known as cybersecurity insurance or cyber liability insurance, is designed to help mitigate the potential financial losses and liabilities associated with cyber threats and security breaches. It is a wise supplement to a sound cyber strategy. The key purposes of cyber insurance include:

1. **Financial Protection:** Cyber insurance helps cover the costs associated with responding to and recovering from a cyberattack. This may include expenses related to investigation, notification, legal services, and public relations efforts.

2. **Liability Coverage:** It provides coverage for legal liabilities that may arise if sensitive information is compromised, leading to lawsuits or regulatory fines. This can include costs associated with legal defense and settlements.

3. **Business Interruption Coverage**: Cyber insurance can offer coverage for loss of income or extra expenses incurred due to a cyber incident that disrupts normal business operations.

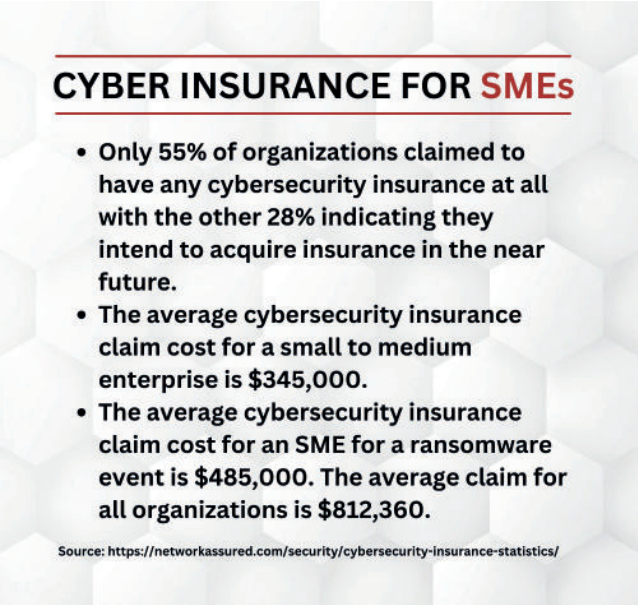
4. **Risk Management Support**: Some policies may include risk management services and resources to help organizations assess and improve their cybersecurity posture, potentially reducing the likelihood of incidents.

5. **Data Breach Response**: Cyber insurance often covers the costs associated with notifying affected individuals, credit monitoring services, and other responses necessary to manage a data breach.

6. **Reputation Management**: In the aftermath of a cyber incident, the insurance may assist with public relations efforts to manage and restore the organization's reputation.

7. **Regulatory Compliance**: Cyber insurance can assist in covering the costs of compliance with data protection regulations and requirements.

Given the increasing frequency and sophistication of cyber threats, cyber insurance has become an essential component of risk management for businesses and individuals relying on digital systems and data. It helps to transfer some of the financial



risks associated with cyber incidents to an insurance provider, providing a layer of financial protection against the potential consequences of a cyberattack.

Your Technology Partner Can Make Assessments & Recommendations

Before issuing a cyber policy, every insurance company will want an assessment of your current systems and processses. Your technology partner can be an invaluable resource for this process. They can pre-emptively integrate basic cyber protections and policies to help you qualify for the best premium. They are often utilized by the insurance company as a resource, so be sure you're working with a credible partner. Conscious Networks does not sell cyber insurance, but we work with trusted partners who can provide options to consider.

Top 4 The Questions About Cyber Insurance

Every business should consider cyber insurance coverage to protect your daily operations, intellectual property, and data if and/or when an attack occurs. Here are some of the common questions we hear:

1. **What does cyber insurance cover?** Cyber insurance can help cover and negate the costs associated with a cyber-attack, litigation costs, fines, and penalties. It is also a requirement for any business who must maintain compliance for certain industries and government entities.

2. **How Much Coverage Do I Need?** Determining the appropriate amount of coverage is a critical concern. Businesses want to ensure they have adequate protection without overpaying for unnecessary coverage. Factors influencing the coverage amount include the size of the business, the industry, the type of data handled, and the potential financial impact of a cyber incident. An accurate risk assessment is essential for tailoring the coverage to the business's unique needs.

3. **Are there cyber insurance discounts available?** Many cyber insurance companies provide a questionnaire to evaluate cyber risk, the current prevention strategies that are in-place, and the level of ongoing support and oversight that your company employs to prevent attacks. Even a basic cybersecurity plan can reduce your overall risk and potentially lower your premiums.

4. **Are employee-induced cyber threats covered by cyber insurance?** A large portion of cyber threats are unintentionally caused by employees. Employees may inadvertently launch malware, respond to phishing incidents, or expose your network to attacks via their tablets and cell phones. Endpoint security, employee training, and malware prevention can be effective tools to curb these threats. Cyber insurance can also help you if one of these types of attacks occurs.

HOLD FOR ADDITIONAL CONTENT?

Our Conscious Approach to Technology

What does a conscious approach to technology mean? Well, this guide is a great example. We have seen many challenges and experiences with cyber security. Our goal is to educate and inform you so that you can make better decisions when it comes to your business technology and cyber security.

Along the way, we have learned valuable lessons about cyber insurance. So, while our organization does not sell cyber insurance, we thought it would be helpful to provide a background on why cyber security and cyber insurance go hand in hand. That's a holistic approach.

In addition, we understand that the biggest challenge to integrating new technology in any business is understanding that not all technology results in more productivity or return on investment. We recognize that one technology decision can have a ripple effect on your business – good or bad. So, our technology advisors help businesses make better technology decisions that seamlessly integrate with your users, your clients, your infrastructure, and your business operations. We serve as technology advisors, first and foremost, while providing a wide array of technology services. Most of all, we help protect your business' most valuable asset - your data!

How Our Team Helps Customers

- EXPERTISE: Conscious Networks provides you with a deep team of professionals, that have specialized expertise. It allows businesses to tap into a plethora of experience that would be nearly impossible to duplicate in-house.
- PROVEN SOLUTIONS: Customers benefit from a focus on sustainable solutions in what is unfortunately, frequently, a band-aid-driven industry of temporary patchwork fixes.
- HARDENED ENVIRONMENTS: Data center, cloud, managed services, and connectivity services are hosted and managed in one of the world's premier data centers, providing unsurpassed security and resiliency.
- OPERATIONAL EXPERTISE: Customers benefit from a commitment to industry best practices and high standards, supplemented with the knowledge of a staff averaging over 14 years each of professional technology experience.
- THE LATEST KNOWLEDGE: You benefit from a team of professionals constantly networking with other uptime, connectivity, and security experts to share and obtain knowledge of the latest security protocols and best practices for uptime and availability.

Contact us today to start the conversation.

Visit: Conscious.net

conscious NETWORKS Conscious.net

TECHNOLOGY IN YOUR OFFICE	TECHNOLOGY BEYOND YOUR OFFICE	END-TO-END TECHNOLOGY ADVISORS
HARDWARE & SOFTWARE SUPPORT	COLOCATION	IT OUTSOURCING
HELP DESK	DATA CENTER	IT MANAGED SERVICES PROVIDER
24/7 NETWORK MONITORING	HELP DESK	IT ARCHITECTURE & CONSULTING
BACKUP & RECOVERY SYSTEMS	24/7 NETWORK MONITORING	INFRASTRUCTURE ANALYSIS
MANAGED DESKTOP	CLOUD DATA MANAGEMENT	APPLICATIONS & PROCESSES
IAAS: INFRASTRUCTURE AS A SERVICE	WEBSITE & EMAIL HOSTING	SOFTWARE & HARDWARE ADVISORS
	BACKUP & RECOVERY SYSTEMS	HELP DESK
	VIRTUAL PRIVATE SERVERS	COMPLIANCE
	DAAS: DESKTOP AS A SERVICE	EQUIPMENT & SOFTWARE ACQUISITION
	MDR & ENDPOINT SECURITY	

Get Started Today!

SCHEDULE NOW

Conscious.net