DEFENDING THE DIGITAL REALM:

FTC SAFEGUARDS AND AFFECTED COMPANIES CHANGED JUNE 2023
IS YOUR COMPANY AFFECTED?
ARE YOU PREPARED?
IN A HURRY? SKIP TO PAGE 7!

A Comprehensive Guide to Cybersecurity Risk Assessment

TODD THORSON
CIO, CTO, CISO
TANJ Cybersecurity & Technology
tthorson@tanjtech.com

CHAPTER 1:
Understanding Cybersecurity Risk Assessment

Picture this: a grand puzzle where every piece represents a potential threat to your business. Cybersecurity risk assessment is the map that helps you navigate through this puzzling landscape. It's like having Sherlock Holmes on your side, but without the funny hat.

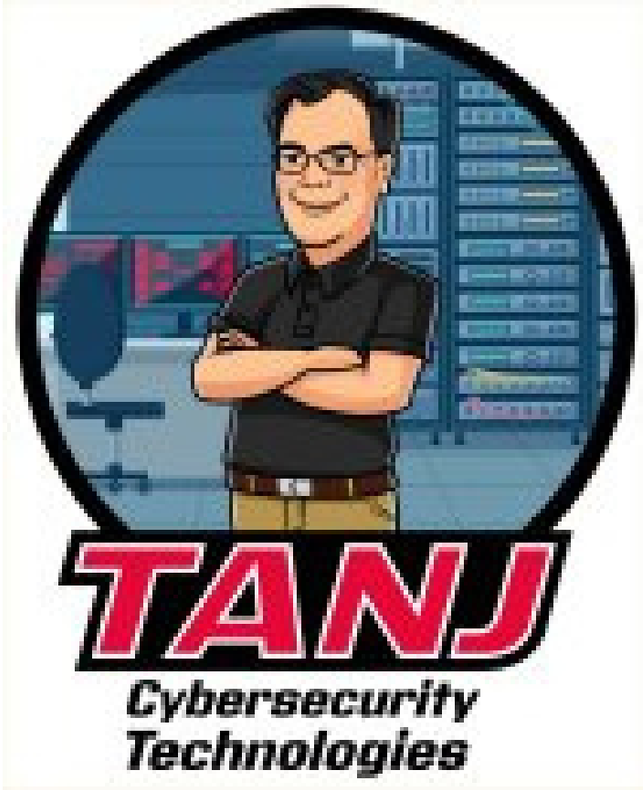
In this chapter, we'll explore the fundamentals of cybersecurity risk assessment and its significance in protecting your business. Let's dive deeper into the world of risk assessment with a real-world case study.

Case Study: The Hotel Hack

Imagine you're the owner of a luxurious hotel, catering to high-profile guests from around the world. Your business relies heavily on online bookings and payment systems. One fateful day, you wake up to discover that your hotel's systems have been compromised, leaving guest data exposed and online transactions compromised.

This real-life case involves a hotel chain that suffered a cyberattack due to insufficient risk assessment. The attackers exploited vulnerabilities in the hotel's online booking platform, gaining access to sensitive customer information, including credit card details. The fallout was catastrophic, resulting in reputational damage, financial losses, and lawsuits from affected customers.

Had the hotel conducted a thorough cybersecurity risk assessment, they could have identified and addressed the vulnerabilities in their online systems, preventing the devastating breach. The lesson here is clear: risk assessment is not a luxury; it's a necessity for businesses of all sizes and industries.



39 seconds

between each successful cyber attack in the United States
THINGS HAVE CHANGED.

CHAPTER 2:
Identifying Cybersecurity Risks

Time to put on your detective hat! We're on the hunt for cyber threats that could sink your ship faster than a fleet of pirates. From malicious malware to cunning phishing schemes, we'll explore the dark corners of the internet where these scoundrels hide.

In this chapter, we'll dive into various types of cyber threats and vulnerabilities that businesses face. Let's examine a real-world case study to understand the implications of overlooking these risks.

Case Study: The Retail Ransomware Ruckus

Imagine you own a thriving retail business with an online presence. Your e-commerce website serves as a vital revenue stream, handling customer transactions and storing sensitive personal data. One unfortunate day, you receive a menacing email from an unknown source, claiming to have encrypted all your website's data and demanding a hefty ransom to restore access.

This case study revolves around a retail company that fell victim to a ransomware attack due to inadequate risk identification. The attackers exploited a vulnerability in the website's outdated software, gaining unauthorized access and encrypting critical data. The company faced significant financial losses, reputational damage, and disruptions to their operations, all because they underestimated the importance of identifying and mitigating cyber risks.

By conducting a comprehensive risk assessment, the retail business could have proactively identified the vulnerability, applied necessary security patches, and implemented robust backup mechanisms to mitigate the impact of such an attack.

Remember, in the world of cybersecurity, knowledge is power. Identifying potential risks is the first step in fortifying your business against the cunning tactics of cyber villains.

CHAPTER 3:
Assessing Risk Impact and Likelihood

It's time to crunch some numbers and determine the probability of your business falling prey to these digital monsters. We'll dive into the nitty-gritty of quantitative and qualitative assessments, but don't worry—we promise not to subject you to complex mathematical equations. No calculus required!

In this chapter, we'll explore different methods for assessing the impact and likelihood of cyber risks. Let's examine a real-world case study that highlights the significance of understanding risk impact.

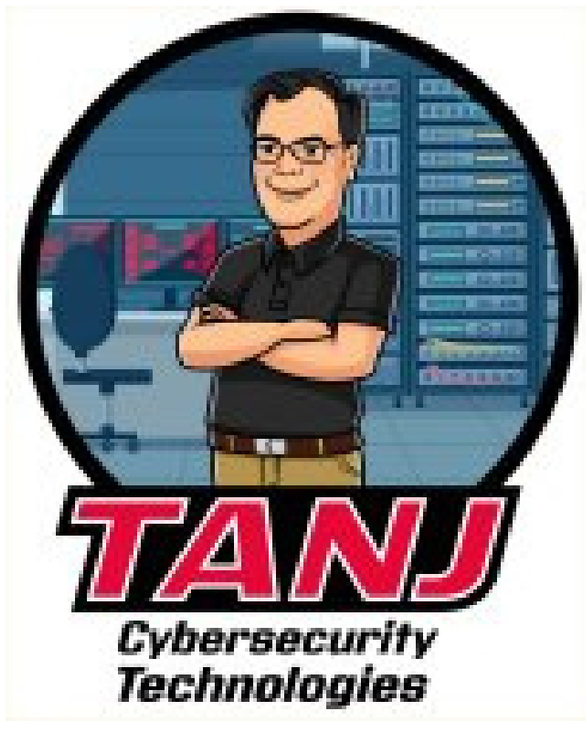
Case Study: The Healthcare Data Breach

Imagine you're the manager of a medical clinic, responsible for handling sensitive patient records and ensuring their confidentiality. One unfortunate day, you discover that a cybercriminal gained unauthorized access to your clinic's database, compromising the personal health information of hundreds of patients.

The attackers exploited vulnerabilities in the clinic's outdated software, accessing patient records and potentially exposing sensitive medical information. The fallout was not only detrimental to the clinic's reputation but also posed serious risks to patient privacy and trust.

Had the clinic conducted a comprehensive risk assessment, they could have recognized the potential impact of a data breach on their business and the lives of their patients. By understanding the value and sensitivity of the data they held, they could have implemented appropriate security measures such as encryption, access controls, and regular software updates to mitigate the risk.

Remember, risk assessment is not just about identifying risks; it's also about evaluating their potential consequences. By understanding the impact and likelihood of cyber risks, you can make informed decisions and allocate resources effectively to protect your business.



$27 Million

stolen each day in The United States.
THINGS HAVE CHANGED.

CHAPTER 4:
Prioritizing and Managing Risks

Just like juggling flaming torches while riding a unicycle, managing cybersecurity risks requires skill and precision. We'll help you prioritize those risks and develop a battle plan to protect your assets. Get ready to show those cyber-crooks who's boss!

In this chapter, we'll delve into strategies for prioritizing and managing cybersecurity risks. Let's explore a case study that demonstrates the importance of risk management in mitigating potential threats.

Case Study: The Financial Firm's Phishing Fiasco

Imagine you're the CEO of a prestigious financial firm that handles vast amounts of sensitive client information and conducts critical financial transactions. One sunny morning, chaos ensues as employees fall victim to a well-crafted phishing email, leading to unauthorized access to confidential client data and potential financial fraud.

This real-life case involves a financial firm that suffered a significant breach due to insufficient risk management practices. The attackers exploited human vulnerabilities by using sophisticated phishing techniques to trick employees into divulging their login credentials. The firm faced severe financial and reputational damage, not to mention potential legal implications.

By implementing robust risk management strategies, such as employee awareness training, multi-factor authentication, and email filtering systems, the financial firm could have significantly reduced the likelihood and impact of such a phishing attack. It's crucial to prioritize risks based on their potential consequences and develop comprehensive risk mitigation plans tailored to your organization's needs.

CHAPTER 5:
Compliance and Regulatory Considerations

Ah, the ever-present specter of compliance. It may seem like navigating a labyrinth of legal jargon, but fear not! We'll guide you through the maze of cybersecurity regulations and standards, helping you stay on the right side of the law while fortifying your defenses.

In this chapter, we'll explore the intersection of cybersecurity risk assessment and regulatory compliance. Let's examine a case study that emphasizes the importance of aligning risk assessment practices with industry regulations.

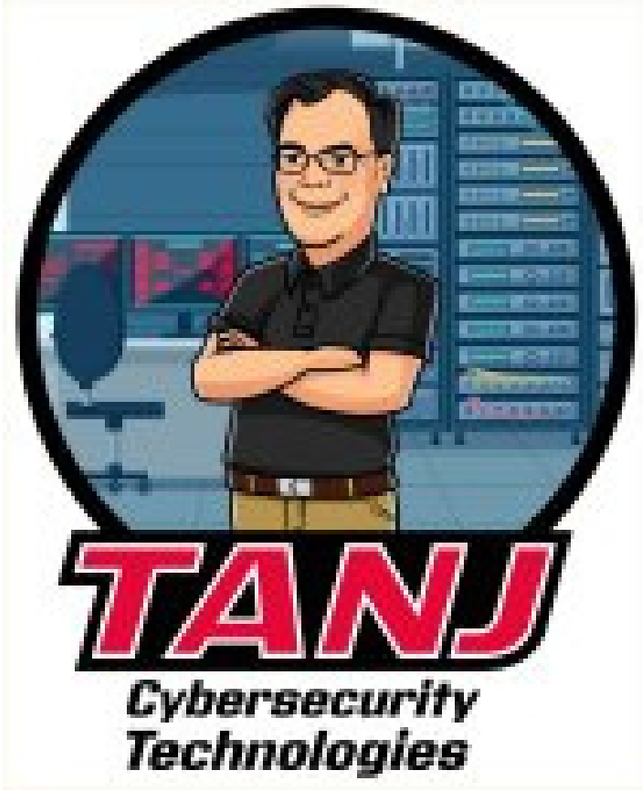
Case Study: The Data Protection Dilemma

Imagine you're the owner of a technology startup that handles vast amounts of personal data from your users. One day, you receive a notice from the data protection authority, stating that your company is under investigation for potential violations of data privacy regulations. Panic ensues as you realize that you have not implemented adequate safeguards to protect user data.

The company failed to implement necessary security controls and safeguards, leaving user data vulnerable to unauthorized access. As a result, they faced severe penalties, loss of customer trust, and potential legal consequences.

By integrating compliance considerations into their risk assessment framework and diligently adhering to data privacy regulations, the startup could have avoided such a predicament. Understanding and addressing regulatory requirements not only protect your business from penalties but also enhance your overall cybersecurity posture.

Remember, compliance is not just a box to check; it's a critical aspect of safeguarding your business and earning the trust of your customers.



>50%

of all cyber attacks are aimed at small businesses.
THINGS HAVE CHANGED.

CHAPTER 6:
Continuous Monitoring and Improvement

Picture your business as a well-fortified castle, complete with a moat and drawbridge. But even the sturdiest castles need vigilant guards to keep watch. We'll explore the importance of ongoing monitoring and assessment, ensuring your defenses stay strong against the evolving tactics of cyber miscreants.

In this chapter, we'll emphasize the need for continuous monitoring and improvement in your cybersecurity risk assessment practices. Let's delve into a case study that illustrates the consequences of neglecting this crucial aspect.

Case Study: The Manufacturing Meltdown

Imagine you're the operations manager of a manufacturing company renowned for producing cutting-edge technology products. As your business expands and embraces digital transformation, the interconnectedness of your systems also increases. However, due to budget constraints and a lack of proactive monitoring, you fail to detect a critical vulnerability in your production line.

This real-life case involves a manufacturing company that experienced a significant security breach due to a lack of continuous monitoring. Attackers exploited a vulnerability in the company's Internet of Things (IoT) devices, gaining unauthorized access to the production line. The breach led to production disruptions, compromised product quality, and financial losses.

By implementing a robust monitoring system that includes real-time threat detection, network monitoring, and system log analysis, the manufacturing company could have identified and mitigated the vulnerability before it was exploited. Ongoing monitoring and improvement are essential to stay one step ahead of cyber threats in the ever-evolving digital landscape.

74%

number of cyber insurance claims being denied in 2023

THINGS HAVE CHANGED.

Are you following FTC Safeguards in your business?

If not, you are risking fines, penalties, financial theft, and the reputation damage that comes with a breach.

In 2021 The Federal Trade Commission (FTC) announced an amendment to the Standards for Safeguarding Customer Information (Safeguards Rule), stating all institutions “engaging in financial activities” must strengthen their cybersecurity practices to better protect customer data. This took effect in June 2023 and currently they are targeting and penalizing car dealerships, mortgage brokers, and other financial "connectors" as cybercrime is at an all time high. Your current IT staff should be aware of these changes and already implemented a plan to protect your company.

The Safeguards Rule requires you to develop, implement, and maintain an information security program with administrative, technical, and physical safeguards designed to protect customer information. Your information security program must be written and appropriate to the size and complexity of your business, the nature and scope of your activities, and the sensitivity of the information at issue.

The objectives of your company’s program are:
• to ensure the security and confidentiality of customer information;
• to protect against anticipated threats or hazards to the security or integrity of that information
• to protect against unauthorized access to that information that could result in substantial harm or inconvenience to any customer.

Questions? The TANJ CSRA (Cyber Security Risk Assessment) can make sure you are compliant to avoid fines and penalties.

info@tanjtech.com
www.tanjtech.com

Book a strategy session! - scan the QR or meetup.tanjtech.com

A SMALL EXCERPT FROM THE AMENDED RULES

- Conduct a written risk assessment that includes risk criteria and how your business cybersecurity program will address and mitigate risks.
- Conduct additional periodic risk assessments.
- Create and document an incident response plan containing goals, communications plan, processes, and roles/responsibilities.
- Designate or hire a “qualified individual” to oversee your businesses cybersecurity program.
- Conduct and document a data and system inventory of all information your business collects, stores, or transmits.
- Provide annual reports to the board of directors on compliance and cyber hygiene status.
- Ensure encryption of all customer information in transit and at rest, document retention and disposal procedures for customer information.
- Enable Multi-Factor Authentication (MFA) for all systems containing customer’s sensitive information.
- Establish change management procedures for modifying information systems.
- Implement policies, procedures, and controls to monitor and log activity.
- Provide annual reports to the board of directors on compliance and cyber hygiene status.

Can this happen at my business?

Consider how money and sensitive information moves around your business. Is a hacker watching this to determine the best way to steal it? How would you know? This story is taken from a real world example, names changed for privacy.

Suzy works in the office at ACME car dealer and is responsible for processing auto payoffs on trade-ins. A hacker has been in their systems silently for 30 days watching everyone's emails, systems accessed, and collecting client information, email signatures, forms, and banking information along with exfiltrating the data for sale on the dark web A client trades in their old car on a new one. Suzy initiates a payoff via bank check using their standard form and files the paperwork. The exact amount was removed from the bank account so everything balances. What everyone doesn't know is that the hacker redirected the funds to an offshore account. No one knows anything until 30 days later the bank is calling the client asking why they haven't made their car payment. The customer contacts the car dealer, and the dealer has to again payoff the car for the customer. It takes 3 months to figure out what happened and was a serious impact to the dealership operations costing several hundred thousand dollars.

According to the FTC, businesses that fall under their new umbrella that do not comply with the Safeguards Rule can face hefty fines and penalties. The maximum fine you can incur is $11,000 per day per occurrence of a breach, and the FTC can seek damages for consent violations which could total over $43,000 per day for each violation. The FTC may also initiate an investigation into the your companies data security practices, which could result in additional penalties, interruption, and damage to the business reputation. The maximum fine for non-compliance is $46,517 per incident.

CHAPTER 7:
Partnering for Success - The MSP Advantage

Congratulations on your journey to understanding the importance of cybersecurity risk assessment and fortifying your business against digital threats.

As a trusted Managed Services Provider (MSP) committed to helping businesses like yours fortify their cybersecurity defenses, we stand ready to guide you in assessing risks, mitigating breaches, and navigating compliance penalties. Allow us to shed light on the advantages of partnering with an MSP like TANJ Cybersecurity & Technology to achieve cybersecurity excellence.

Expertise and Experience: At TANJ Cybersecurity & Technology, we specialize in cybersecurity, possessing a wealth of knowledge and experience in assessing risks and implementing effective security measures. By partnering with us, you gain access to a dedicated team of professionals well-versed in the latest threats and best practices. Our expertise becomes your competitive advantage.

Comprehensive Risk Assessment: Our robust tools and methodologies enable us to conduct thorough risk assessments tailored to your business. We identify vulnerabilities, analyze potential impacts, and recommend targeted strategies to mitigate risks. With our assistance, you can uncover blind spots and ensure a holistic approach to safeguarding your organization.

Proactive Threat Monitoring: Cyber threats are relentless and ever-evolving. With our advanced threat detection systems and round-the-clock monitoring, we offer proactive monitoring services to detect and respond to potential breaches swiftly. Our real-time insights keep you ahead of attackers, ensuring proactive defense.

Rapid Incident Response: In the unfortunate event of a cybersecurity incident, time is of the essence. Equipped with incident response capabilities, we help you mitigate the impact, minimize downtime, and swiftly restore normal operations. Our expertise in handling incidents ensures a coordinated and efficient response, reducing the potential damage to your business.

Compliance Guidance: Navigating the complex landscape of cybersecurity regulations and compliance requirements can be daunting. At TANJ Cybersecurity & Technology, we excel in providing guidance and support, ensuring your organization meets regulatory obligations. We help you develop and implement security controls aligned with relevant frameworks, protecting you from potential penalties and legal consequences.

Scalability and Cost Efficiency: As your business evolves, so do your cybersecurity needs. With our scalable solutions, you can adjust your security measures seamlessly. By partnering with TANJ Cybersecurity & Technology, you gain access to robust cybersecurity services without the need for significant upfront investments in infrastructure and specialized personnel. We offer cost-effective solutions that grow alongside your organization.

info@tanjtech.com
www.tanjtech.com
Book a strategy session! - scan the QR or meetup.tanjtech.com

CONCLUSION

As a visionary business leader, you understand the importance of fortifying your business against cyber threats. Partnering with TANJ Cybersecurity & Technology empowers you with the expertise, comprehensive risk assessment capabilities, proactive monitoring, rapid incident response, compliance guidance, and scalability needed to elevate your cybersecurity posture.

Embrace the power of collaboration and forge a partnership with TANJ Cybersecurity & Technology to thrive securely in the digital realm. Together, we can navigate the ever-changing cybersecurity landscape, emerging stronger than ever before.

Stay vigilant, adapt to emerging threats, and let the expertise of TANJ Cybersecurity & Technology be your shield against cyber breaches and compliance penalties. We are committed to safeguarding your business and ensuring your success in the face of cyber adversaries.

With TANJ Cybersecurity & Technology as your trusted ally, you can focus on what you do best while we protect your organization's digital assets. Contact us today, and let us embark on this cybersecurity journey together.

TANJ
CYBERSECURITY
TECHNOLOGY

Technology Services

TANJ Technologies

We make IT happen

www.tanjtech.com
(630) 617-5330

Notes, Thoughts, Questions

info@tanjtech.com
www.tanjtech.com

Book a strategy session! - scan the QR or meetup.tanjtech.com

Homework

How will you assess and mitigate your risk?

1) Think about everyone in your network - family, friends, neices, nephews, kids, grandkids, anyone that could possibly ever call your for money. Think of a word, phrase, or event that only the real person would know. If (when) you get a call that could be from a hacker, ask for that word, phrase, or event to validate the person. AI will make it almost impossible to tell the voice (or video!) from the person you know. Do this ahead of time, it will be too hard to think in the moment when it happens. Be ready! Please dont be the next victim!

49%

Year over year revenue increase of hacking companies and bad actors

THINGS HAVE CHANGED.

What will happen if you do nothing?

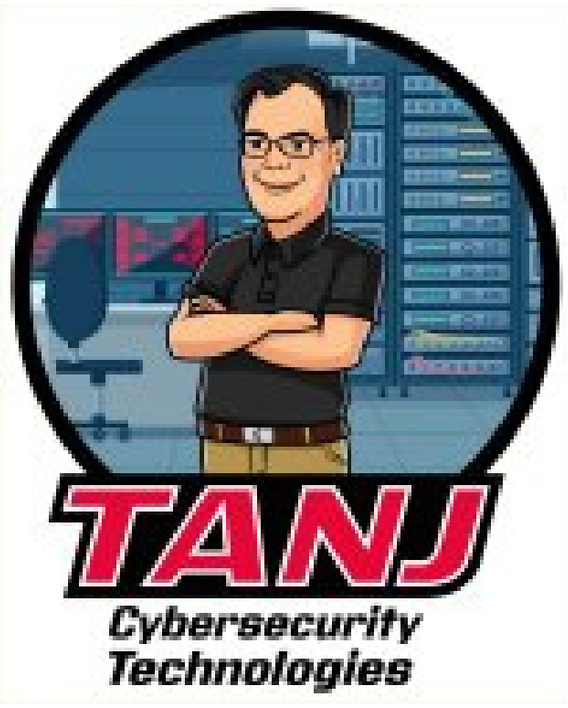
TANJ

CYBERSECURITY
TECHNOLOGY

90%

of cybersecurity events are started by internal employees either accidentally or purposefully.
THINGS HAVE CHANGED.
How long will you wait to take action?

info@tanjtech.com
www.tanjtech.com
Book a strategy session! - scan the QR or meetup.tanjtech.com



info@tanjtech.com

Technology Services

TANJ Technologies
We make IT happen

www.tanjtech.com
(630) 617-5330