# Steering Clear of Cyber Risks:
# Securing Your Company in the Digital Age

ISACA San Diego Chapter

FRSECURE

TRUCKING PROUD INSURANCE AGENCY

Cyber Center of Excellence

C3

California Trucking Association

We drive for a living. Safety is our priority.

August 22ND 2023 Hosted by Joe Erle & Dave Tuckman

# Who Is Joe Erle?

Here's information about Joe. Don't worry – we don't spend a lot of time on these slides…

## Professional Summary

- 15+ years experience in commercial insurance working with IT & Cybersecurity, Industries.
- Founding member of C3 Risk & Insurance
- Agency of the year winner
- Certified Risk Manager (CRM)
- Certified Insurance Counselor (CIC)
- Trusted Risk Advisor (TRA)
- MBA in business administration with a concentration on tech project management

## Community Service

- Soccer and baseball coach

## Links

- LinkedIn: https://www.linkedin.com/in/joeerle
- Discover the Difference Podcast: https://youtu.be/TBbfzTjf8IY
- Website: www.c3insurance.com
- Joe's YouTube: https://www.youtube.com/@notyouraveragejoesinsuranc6442

## Certifications

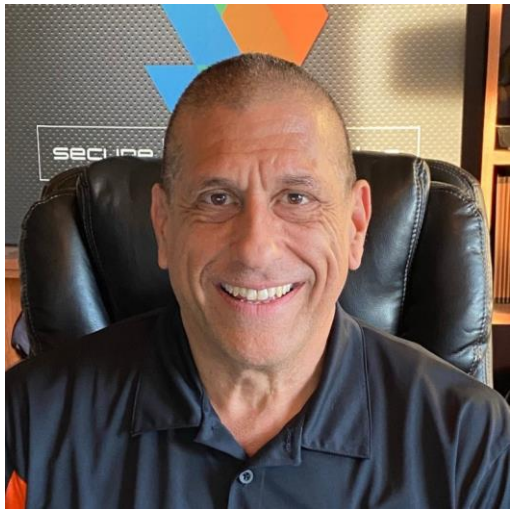
Trusted Risk Advisor™
Consulting→Diagnosing→Protecting

# Who Is Dave (Tuckman)?

Here's information about me. Don't worry – we don't spend a lot of time on these slides…

## Professional Summary

- 30+ years leadership, management, and executive level experience in the IT & Cybersecurity, Industries.
- Founded, developed, managed, and sold two business (technology services, e-commerce website)
- Experience building security and compliance, programs based on NIST CSF, NIST RMF, CMMC/NIST 800-171, CIS-18, HIPAA, PCI, and other frameworks.
- Experience in performing assessments using, HIPAA, NIST CSF, CIS-18, Zero Trust and other frameworks.
- Presently Information Security Consultant at FRSecure, working to help fix a broken industry.
- Working on a publication: 100 Pieces of Advice for 100 CISOs



## Community Service

- Currently serve as chapter President for ISACA San Diego.
- Member of (ISC)2, ISACA, ISSA, IAPP, Infragard
- Recognized public speaker. mentor, mentee, and contributing member of the local InfoSec community.

## Links

- LinkedIn: https://www.linkedin.com/in/davetuckman/
- ISACA San Diego: https://isaca-sd.org/board-of-directors
- 100 Pieces of Advice for 100 CISOs: https://www.100cisos.com

## Certifications

C|CISO CERTIFIED CHIEF INFORMATION SECURITY OFFICER
CISM Certified Information Security Manager
CISSP CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL
CDPSE Certified Data Privacy Solutions Engineer
C|EH Certified Ethical Hacker
SECURITYSTUDIO CvCISO CERTIFIED virtual Chief Information Security Officer LEVEL 2
Microsoft 365 CERTIFIED FUNDAMENTALS
Microsoft CERTIFIED SECURITY, COMPLIANCE, AND IDENTITY FUNDAMENTALS
Microsoft CERTIFIED AZURE FUNDAMENTALS
CompTIA Security+

ISACA San Diego Chapter
FRSECURE
TRUCKING PROUD INSURANCE AGENCY
Cyber Center of Excellence
C3
California Trucking Association – We drive for a living. Safety is our priority.

# Securing Your Company in the Digital Age

Complexity Is the Enemy of Security. The more complex a system gets, the harder it is to secure.

## If You Fail to Plan, You Plan to Fail

"If you fail to plan, you plan to fail" means exactly what it says. By failing to plan for a situation, you're basically guaranteeing that you will fail that situation, because you didn't plan for it. **The intent of this presentation is to help you plan.**

# Securing Your Company in the Digital Age

Cybersecurity is like no other industry you will encounter. Those saying it is a broken industry aren't wrong, but we see it more as industry still maturing. And while it has a respectable amount of maturing ahead of itself, it is already a critical part of every organization, its employees, customers, third-parties, and vendors.

## Industry Overview

A high-level look at the Information Security industry, through the lens of the insurance industry.

## Identifying Your Risk

Understanding how to identify risk to your organization. Where to look, and once it's been identified, it can be prioritized.

## Cyber Insurance Checklist

12 (+2) Essential Security Controls

## Resources

Additional resources to support your information security program: Websites, standards/frameworks, templates, tabletop exercises, downloads, Incident Response resources, etc.


ISACA San Diego Chapter · FRSECURE · TRUCKING PROUD INSURANCE AGENCY · Cyber Center of Excellence · C3 · California Trucking Association

# Industry Overview

Learning and innovation go hand in hand. The arrogance of success is to think that what you did yesterday will be sufficient for tomorrow. - William Pollard

## Cyber Insurance Landscape: Trends and Challenges

Underwriting Shifts (2021 Q4 vs. 2023 Q1) / Growing Demand for Coverage

## Navigating Evolving Underwriting Policies

Stricter Coverage and Underwriting / Rising Concerns and Premiums

## Impact of Escalating Cyberattacks

Magnitude of Breaches / Insurer Response and Adjustments

## Strategic Adaptation for Comprehensive Coverage

Evolving Underwriter Expectations / Aligning Strategy with Risk Management

# Industry Overview

Learning and innovation go hand in hand. The arrogance of success is to think that what you did yesterday will be sufficient for tomorrow. - William Pollard

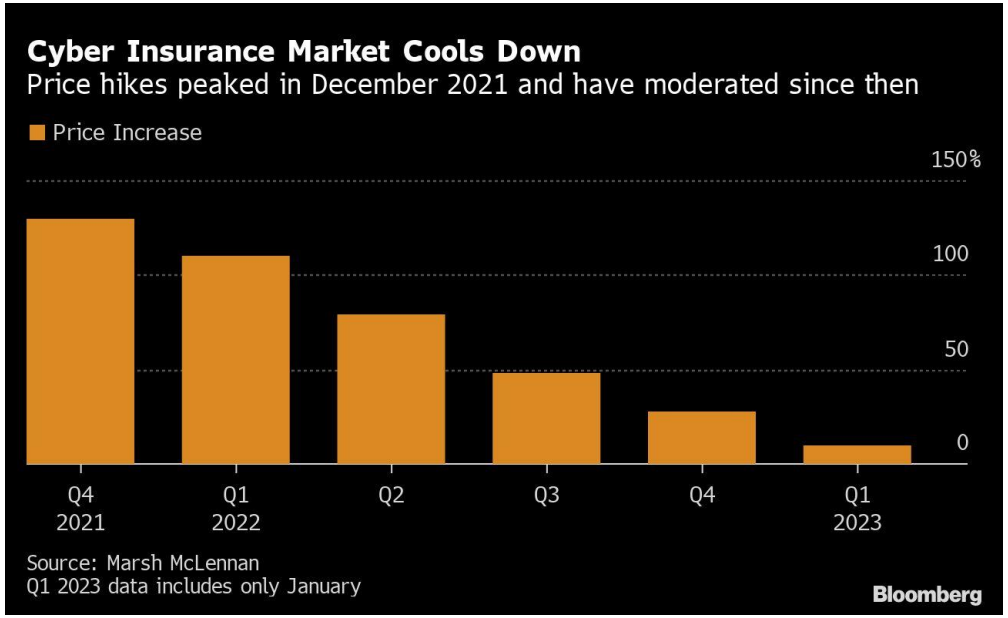
## Cyber Insurance Landscape: Trends and Challenges

**Underwriting Shifts (2021 Q4 vs. 2023 Q1)**

- Primary Premium Trends: Shift from 30-150% increases to flat premiums with some decreases.
- Excess Cover: Easier to obtain, significantly less expensive (65%-80% ILF).
- Retentions/Deductibles: Stable/flat for middle market and Risk Management (RM) clients.
- Co-Insurance: Reduced usage and percent among new entrants; often industry-specific.

**Growing Demand for Coverage**

- 48% already invested in cyber insurance for identity-related incidents.
- 32% planning to invest, reflecting rising breach concerns.



# Industry Overview

Learning and innovation go hand in hand. The arrogance of success is to think that what you did yesterday will be sufficient for tomorrow. - William Pollard

## Navigating Evolving Underwriting Policies

**Stricter Coverage and Underwriting**

- Insurers imposing stringent coverage policies and denying claims.
- Organizations facing heightened scrutiny and rigorous underwriting processes.

**Rising Concerns and Premiums**

- Global attacks surged by 38% in 2022 compared to 2021.
- Increased costs for insurers handling cyber claims.
- 2022 witnessed higher premiums due to elevated loss ratios.

# Industry Overview

Learning and innovation go hand in hand. The arrogance of success is to think that what you did yesterday will be sufficient for tomorrow. - William Pollard

## Impact of Escalating Cyberattacks

**Magnitude of Breaches**

- 83% of organizations encountered multiple data breaches.
- Average cost of a breach: $9.44M (US), $4.25M (global).
- Stolen credentials and phishing remain top attack vectors.
- Escalating premiums, restricted payouts, and claim denials.

**Insurer Response and Adjustments**

- 27% of data breach claims had policy exclusions.
- Misrepresentations led to the loss of cyber insurance.

# Industry Overview

Learning and innovation go hand in hand. The arrogance of success is to think that what you did yesterday will be sufficient for tomorrow. - William Pollard

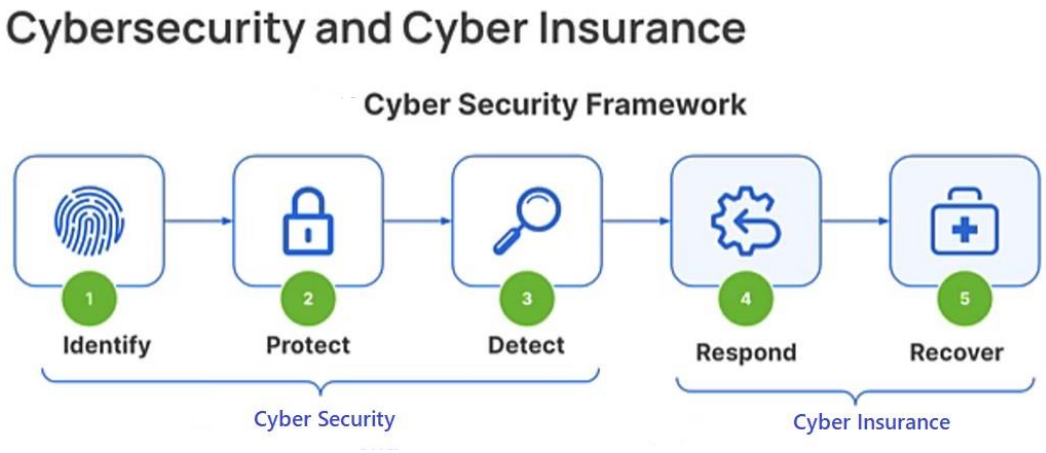
## Strategic Adaptation for Comprehensive Coverage

**Evolving Underwriter Expectations**

- Increasing emphasis on identity protection, authentication, and access controls.
- Compliance with regulations positively influencing coverage terms.

**Aligning Strategy with Risk Management**

- Cyber insurance mitigates ransomware and breach risks.
- Centralizing identity access management and next-gen authentication.
- Staying responsive to evolving underwriting requirements for enhanced coverage.



# Identifying Your Risk

Anyone who stops learning is old, whether at twenty or eighty. Anyone who keeps learning stays young. The greatest thing in life is to keep your mind young. - Henry Ford

## Company

What are my organizations risks, and how can we improve our posture against this risk?

## Customers

What do my customers expect, and what happens if we don't exceed those expectations?

## Competition

What is the competition doing, and how does that impact my relationship(s) with existing and new clients?

## Environment

What do I need to do, to address challenges outside my organization, clients and competition? Think about regulatory changes, the economy, inflation, supply chain vulnerabilities, new technologies, etc.

# 12 (+2) Essential Security Controls

Sun Tzu said **Know the enemy and know yourself in a hundred battles you will never be in peril**. When you are ignorant of the enemy but know yourself, your chances of winning or losing are equal. If ignorant both of your enemy and of yourself, you are certain in every battle to be in peril.

## 0. Know Your Inventory

This is where everything actually starts. We can do any of the other items if we don't know what we have.

**INVENTORY INCLUDES**

- Hardware (workstations, servers, laptops, and mobile devices)
- Software (operating systems, programs, apps, etc.)
- Cloud Services (AWS, Azure, SAAS tools, backups, etc.)
- Data (where is all your data)
- IoT devices (if they connect to the Internet, they connect to the network

**DOCUMENT HOW THEY ARE USED**

- Network Mappings
- Data flow diagrams

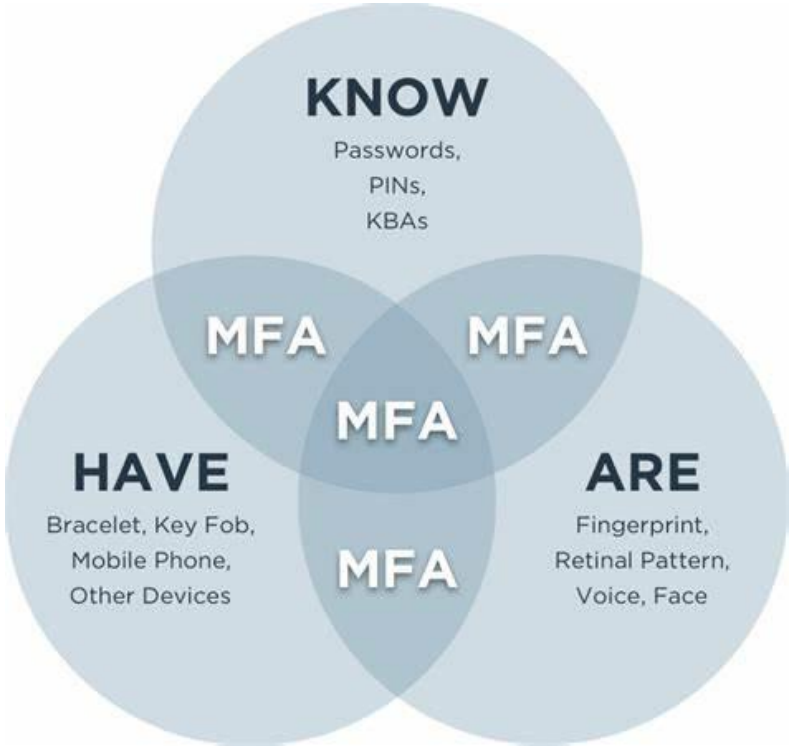
# 12 (+2) Essential Security Controls

Sun Tzu said **Know the enemy and know yourself in a hundred battles you will never be in peril**. When you are ignorant of the enemy but know yourself, your chances of winning or losing are equal. If ignorant both of your enemy and of yourself, you are certain in every battle to be in peril.

## 1. Multifactor Authentication

Ransomware and other attacks frequently exploit weak or stolen passwords to infiltrate systems.

MFA reduces the risk by requiring a combination of verification factors such as a password or PIN along with a security token, mobile app or a biometric identifier. It's almost impossible to get cyber insurance without MFA.




https://www.linkedin.com/pulse/cyber-insurance-checklist-12-essential-security-nilesh

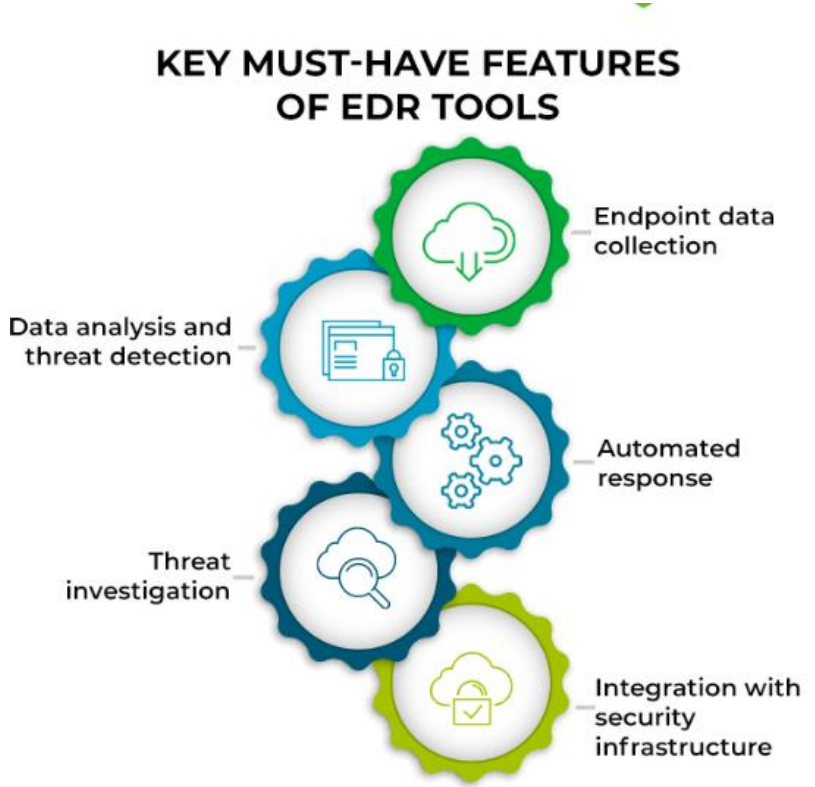
# 12 (+2) Essential Security Controls

Sun Tzu said **Know the enemy and know yourself in a hundred battles you will never be in peril**. When you are ignorant of the enemy but know yourself, your chances of winning or losing are equal. If ignorant both of your enemy and of yourself, you are certain in every battle to be in peril.

## 2. Endpoint Detection and Response

Endpoint devices such as laptops, tablets and mobile phones are enticing targets because they provide a direct route into corporate networks.

Unlike traditional signature-based threat detection tools, EDR solutions use machine learning (ML) and continuous monitoring to identify stealthy threats that lack the usual signs of an infection.




https://www.linkedin.com/pulse/cyber-insurance-checklist-12-essential-security-nilesh

# 12 (+2) Essential Security Controls

Sun Tzu said **Know the enemy and know yourself in a hundred battles you will never be in peril**. When you are ignorant of the enemy but know yourself, your chances of winning or losing are equal. If ignorant both of your enemy and of yourself, you are certain in every battle to be in peril.

## 3. Secure Backups

Many ransomware attacks now target backup data to prevent recovery. Immutable backups that cannot be encrypted, deleted or otherwise modified ensure you have an untouched version of data that is always recoverable.

For additional protection, the immutable backup should be isolated from local systems.


https://www.linkedin.com/pulse/cyber-insurance-checklist-12-essential-security-nilesh

# 12 (+2) Essential Security Controls

Sun Tzu said **Know the enemy and know yourself in a hundred battles you will never be in peril**. When you are ignorant of the enemy but know yourself, your chances of winning or losing are equal. If ignorant both of your enemy and of yourself, you are certain in every battle to be in peril.

## 4. Network Access Controls

Enforce least-privilege access principles to ensure users are limited to only the data and systems access necessary for their jobs.

Identity and access management (IAM) and privileged access management (PAM) solutions deliver strong access controls. IAM solutions provide a framework for verifying user identities, while PAM delivers more control over privileged identities and activities.


https://www.linkedin.com/pulse/cyber-insurance-checklist-12-essential-security-nilesh

# 12 (+2) Essential Security Controls

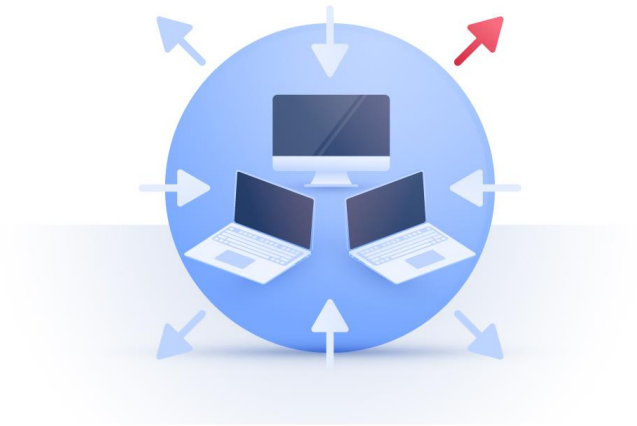
Sun Tzu said **Know the enemy and know yourself in a hundred battles you will never be in peril**. When you are ignorant of the enemy but know yourself, your chances of winning or losing are equal. If ignorant both of your enemy and of yourself, you are certain in every battle to be in peril.

## 5. Filter Content

Content-filtering solutions scan web applications, identify malware signatures, and examine text and email messages to protect against data leakage.

**INGRESS**
Data coming into the network

**EGRESS**
Data leaving the network



https://www.linkedin.com/pulse/cyber-insurance-checklist-12-essential-security-nilesh

# 12 (+2) Essential Security Controls

Sun Tzu said **Know the enemy and know yourself in a hundred battles you will never be in peril**. When you are ignorant of the enemy but know yourself, your chances of winning or losing are equal. If ignorant both of your enemy and of yourself, you are certain in every battle to be in peril.

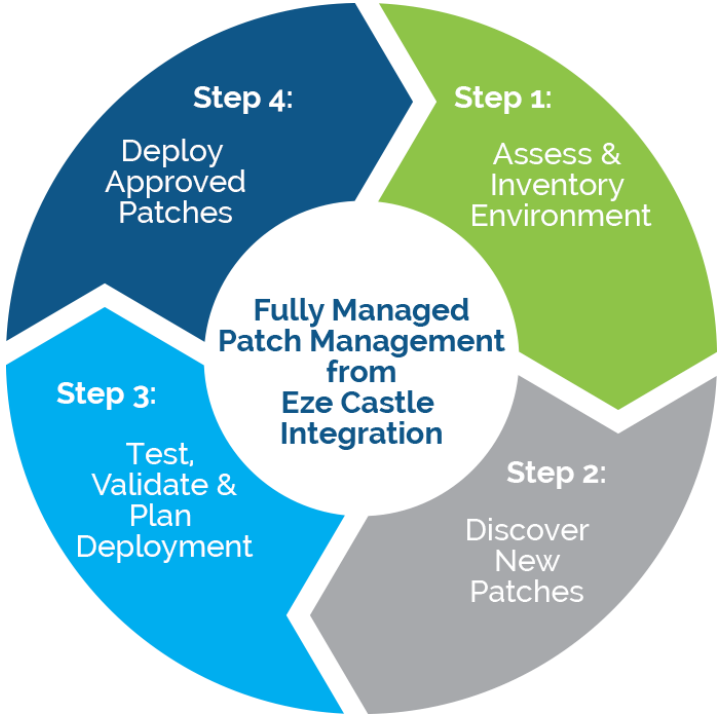
## 6. Vulnerability/Patch Management

A consistent approach to patching and updating software and operating systems helps limit exposure to ransomware and other exploits.

A patch management plan should include a framework for prioritizing, testing and deploying patches.

**CONSIDERATIONS**

- Critical Vulnerabilities/Patches
- Temporary Workarounds
- Employee Awareness and Education




https://www.linkedin.com/pulse/cyber-insurance-checklist-12-essential-security-nilesh

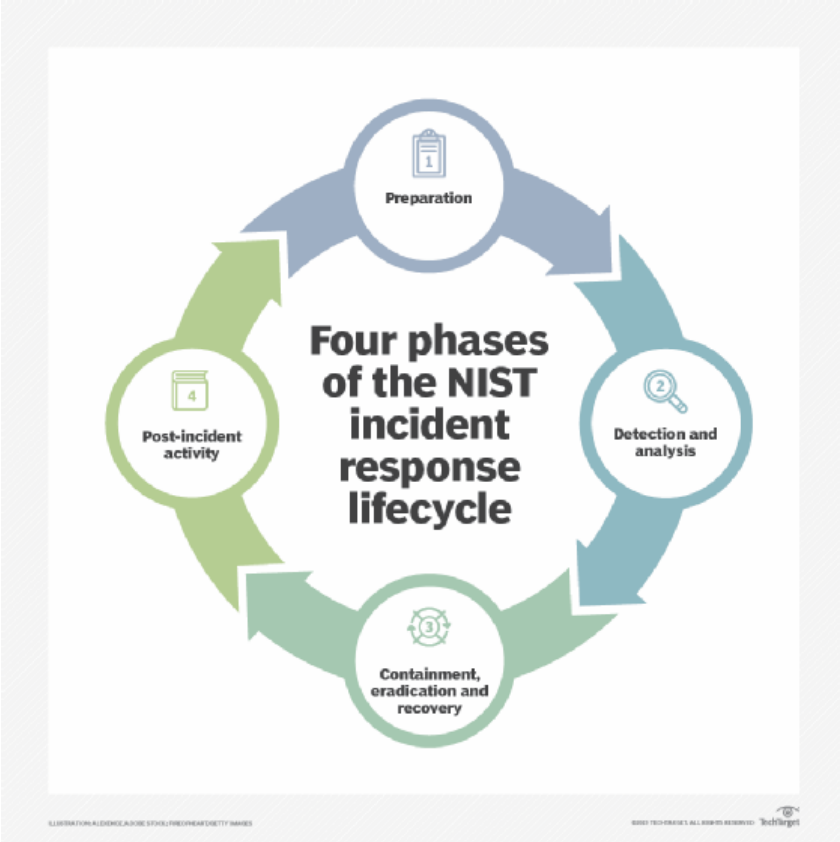
# 12 (+2) Essential Security Controls

Sun Tzu said **Know the enemy and know yourself in a hundred battles you will never be in peril**. When you are ignorant of the enemy but know yourself, your chances of winning or losing are equal. If ignorant both of your enemy and of yourself, you are certain in every battle to be in peril.

## 7. Incident Response Planning

A formal incident response plan should outline specific procedures for detecting, responding to and recovering from a cyberattack.

The plan should describe technical requirements for containing and eradicating threats as well as business requirements for maintaining operations.




https://www.linkedin.com/pulse/cyber-insurance-checklist-12-essential-security-nilesh

# 12 (+2) Essential Security Controls

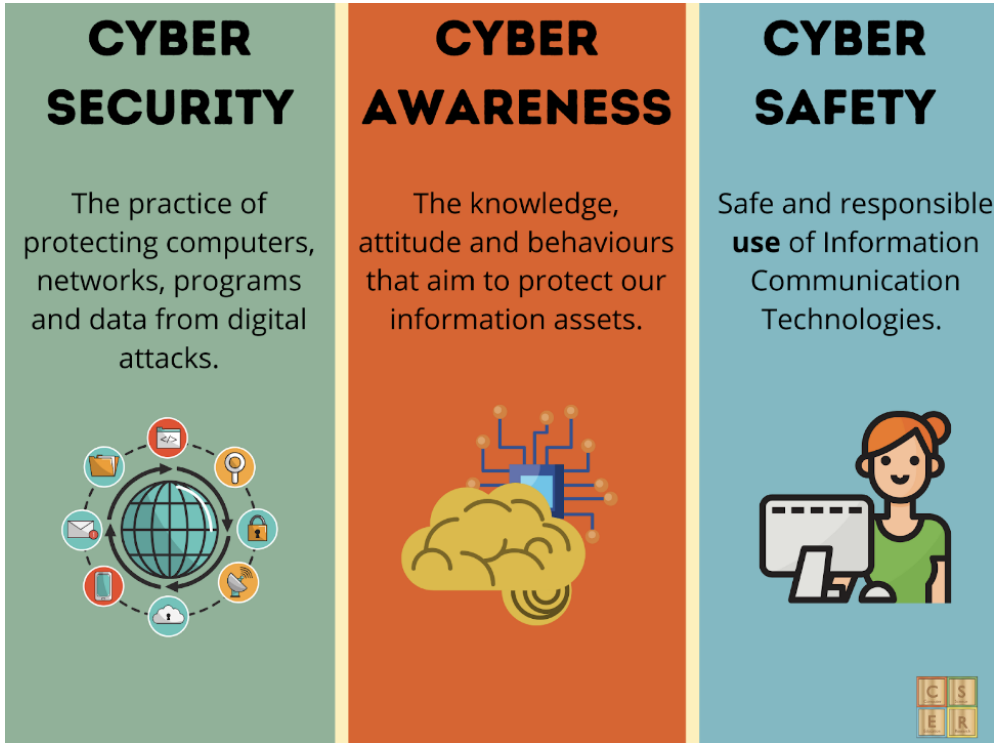
Sun Tzu said **Know the enemy and know yourself in a hundred battles you will never be in peril**. When you are ignorant of the enemy but know yourself, your chances of winning or losing are equal. If ignorant both of your enemy and of yourself, you are certain in every battle to be in peril.

## 8. Cybersecurity Awareness Training

Regular security awareness training promotes general security best practices and an understanding of social engineering and phishing techniques. Users who can spot the telltale signs of an attack can preemptively thwart many attacks.

**GENERAL SECURITY AWARENESS TRAINING**
A focus on general awareness that is applicable to everyone in the organization, its contractors and third parties

**SPECIALIZED AWARENESS TRAINING**
Additional training for those with access to the organization's critical data (executive leadership, finance, system administrators, etc.)




https://www.linkedin.com/pulse/cyber-insurance-checklist-12-essential-security-nilesh

# 12 (+2) Essential Security Controls

Sun Tzu said **Know the enemy and know yourself in a hundred battles you will never be in peril**. When you are ignorant of the enemy but know yourself, your chances of winning or losing are equal. If ignorant both of your enemy and of yourself, you are certain in every battle to be in peril.

## 9. Secure Remote Access

Remote desktop protocol (RPD) enables users to access company resources from a home PC using an Internet connection, but it has known vulnerabilities.

Apply encryption, MFA and other security features to mitigate risk. In addition, block all remote access ports at the firewall or network gateway unless there is a valid business reason for having them open.


https://www.linkedin.com/pulse/cyber-insurance-checklist-12-essential-security-nilesh

# 12 (+2) Essential Security Controls

Sun Tzu said **Know the enemy and know yourself in a hundred battles you will never be in peril**. When you are ignorant of the enemy but know yourself, your chances of winning or losing are equal. If ignorant both of your enemy and of yourself, you are certain in every battle to be in peril.

## 10. Monitor Event Logs

Enable security event logging for all systems, software and endpoint devices, and actively review and analyze those logs to detect attacks and launch countermeasures.

**SIEM**
Solution with the ability to gather security data from multiple information system sources and present that data as digestible, actionable information via a single interface.

**SOC**
A security operations center (SOC) is a command center for the monitoring, analysis and protection from cyber attacks.

**SIEM / SOC AS A SERVICE**
The combination of SIEM and SOC bundled together as a service, transferring the management overhead to a third-party service.


https://www.linkedin.com/pulse/cyber-insurance-checklist-12-essential-security-nilesh

# 12 (+2) Essential Security Controls

Sun Tzu said **Know the enemy and know yourself in a hundred battles you will never be in peril**. When you are ignorant of the enemy but know yourself, your chances of winning or losing are equal. If ignorant both of your enemy and of yourself, you are certain in every battle to be in peril.

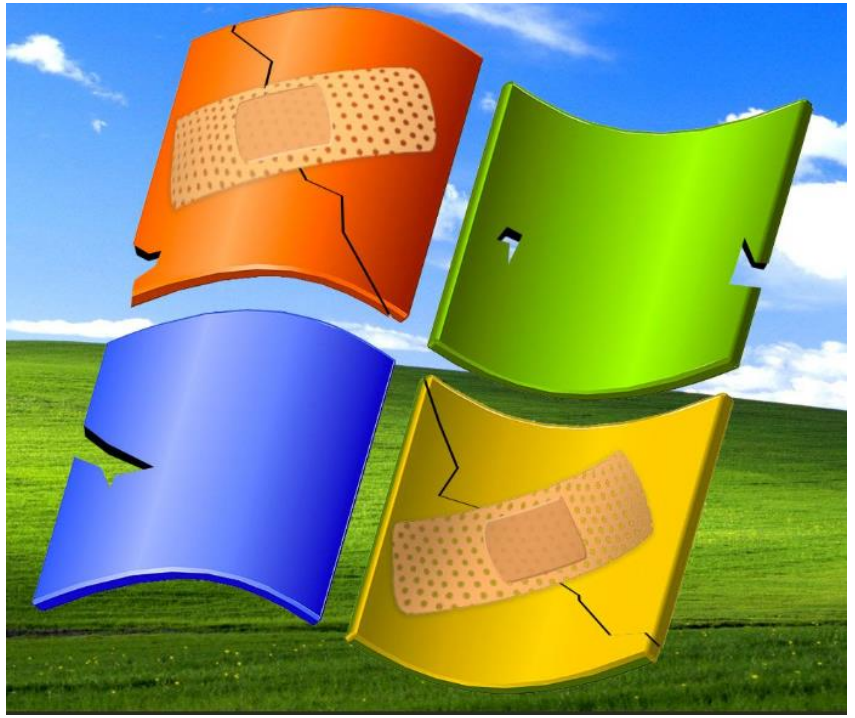
## 11. Replace End-of-Life Systems

Hackers commonly target applications and systems that have reached end of support or end of life because they know security issues are no longer being addressed.

Companies with outdated systems and no plan for upgrades are viewed as poor risks by most insurance underwriters.

**SYSTEM CONSIDERATIONS**

- Computers (servers, workstations, etc.)
- Software (operating systems, vendor software, databases, API's, etc.)
- Network Equipment (firewalls, switches, routers, NAS, etc.)
- IoT Devices (cameras, smart tv, phones, payment terminals, etc.)



https://www.linkedin.com/pulse/cyber-insurance-checklist-12-essential-security-nilesh

# 12 (+2) Essential Security Controls

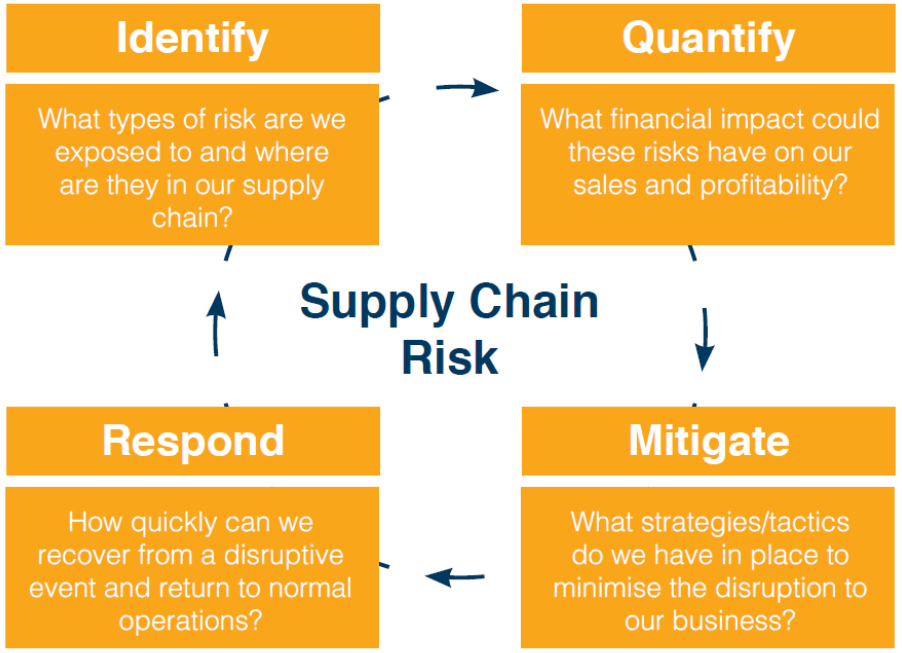
Sun Tzu said **Know the enemy and know yourself in a hundred battles you will never be in peril**. When you are ignorant of the enemy but know yourself, your chances of winning or losing are equal. If ignorant both of your enemy and of yourself, you are certain in every battle to be in peril.

## 12. Manage Supply Chain Risk

Supply chain attacks allow cybercriminals to distribute malware to mass numbers of victims simultaneously. Organizations should evaluate their suppliers' security practices and incorporate specific security requirements into their contracts.

**SUPPLY CHAIN CONSIDERATIONS**

- Partners
- Vendors
- Inventory
- Suppliers (Source materials, parts, components, etc.)
- Labor resources (contractors, shipping providers, etc.
- Professional services (attorneys, financial advisors, outsourced payroll, etc.)
- Other services (housekeeping, etc.)
- Their overall cyber risk exposure (and supply chain risks)




https://www.linkedin.com/pulse/cyber-insurance-checklist-12-essential-security-nilesh

# 12 (+2) Essential Security Controls

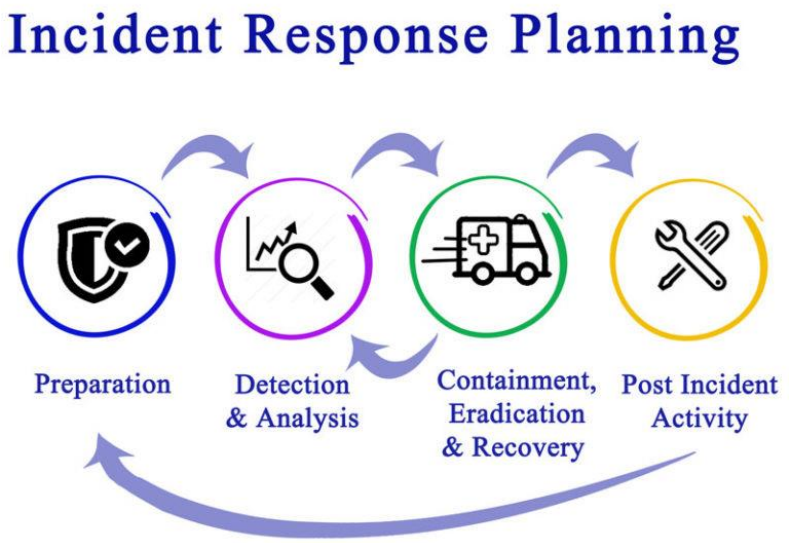
Sun Tzu said **Know the enemy and know yourself in a hundred battles you will never be in peril**. When you are ignorant of the enemy but know yourself, your chances of winning or losing are equal. If ignorant both of your enemy and of yourself, you are certain in every battle to be in peril.

## 13. Know Your Incident Response Procedures

Have a plan for when an incident occurs. Know who your response team is, and everyone's roles and responsibilities.

**PLAN THE WORK, WORK THE PLAN**

- At some point during an incident, your IT and insurance provider will need to collaborate.
- When you get in a car accident, you have the right to choose who repairs the vehicle.
- During negotiations of your policy, work with your provider to clarify how everyone will work together.
- Check for potential overlapping resources. Perhaps you have incident response coverage through another resource.
- Document this plan and its processes.



# Resources

There are some aspects of work you need to keep working on and no matter what environment you are in. Continuous learning is very important. It's what I call 'competitive tension', which is about having a competition around. - Viswanathan Anand

## Information Security Program Resources

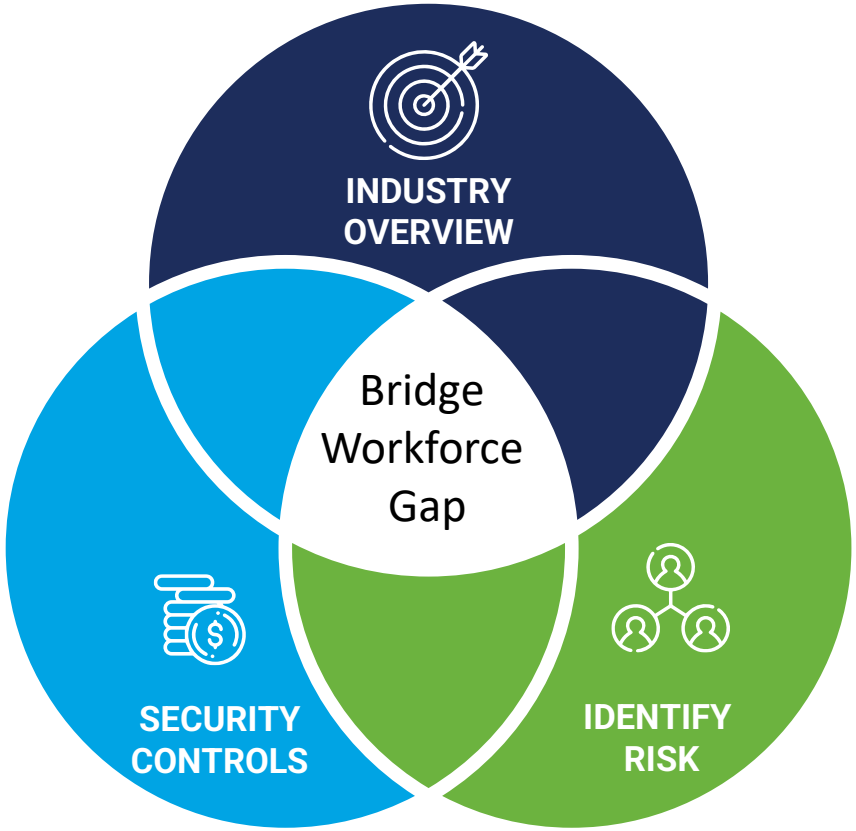
Additional resources to support your information security program: Websites, standards/frameworks, templates, tabletop exercises, downloads, Incident Response resources, etc.

## Information Security Community Resources

Local governmental, private enterprise, non-profit organizational, etc. resources available right here within our local community.

## Incident Response Resources

Resources available in the event of a breach or incident.




ISACA San Diego Chapter · FRSECURE · TRUCKING PROUD INSURANCE AGENCY · Cyber Center CCoE of Excellence · C3 · California Trucking Association "We drive for a living. Safety is our priority."

# Resources

There are some aspects of work you need to keep working on and no matter what environment you are in. Continuous learning is very important. It's what I call 'competitive tension', which is about having a competition around. - Viswanathan Anand

## Information Security Program Resources


- **FRSecure –** https://frsecure.com/resources/
  Information Security experts make available industry recognized cheat sheets, checklists, incident response playbooks, policy templates, program guides, workbooks freely available to everyone.

- **SANS** – SysAdmin, Audit, Network, and Security Institute
  https://www.sans.org/information-security-policy
  SANS has developed and posted a set of security policy templates. Membership to the SANS.org Community grants you access to thousands of free content-rich resources like these templates. Start with the free membership option.

- **NIST** – National Institute of Science And Technology
  NIST develops the cybersecurity standards, guidelines, and resources to meet the standards of U.S. federal, state, local agencies; along with those that wish to do business with must all abide by:
  - NIST Cybersecurity Program History and Timeline
  - NIST SP 800-12 Rev. 1 - An Introduction to Information Security
  - NIST Small Business Cybersecurity Corner
  - NIST Cybersecurity Framework (NIST CSF) / Journey To NIST CSF 2.0
  - NIST Privacy Framework / NIST Risk Management Framework (RMF)

- **CISA** – Cybersecurity & Infrastructure Security Agency
  CISA is the operational lead for federal cybersecurity critical infrastructure security and resilience.
  - Critical Infrastructure Sectors / Free Cybersecurity Services and Tools
  - Cyber Hygiene Services (available to gov services and public/private sector critical infrastructure organizations)

ISACA San Diego Chapter · FRSECURE · TRUCKING PROUD INSURANCE AGENCY · Cyber Center CCoE of Excellence · C3 · California Trucking Association — We drive for a living. Safety is our priority.

# Resources

There are some aspects of work you need to keep working on and no matter what environment you are in. Continuous learning is very important. It's what I call 'competitive tension', which is about having a competition around. - Viswanathan Anand

## Information Security Community Resources


- **Cyber Center of Excellence (CCOE) San Diego**
  https://sdccoe.org
  San Diego-based nonprofit that mobilizes businesses, academia and government to grow the regional cyber economy and create a more secure digital community for all. CCOE's programs and initiatives aim to increase regional cyber resiliency, seed and diversify the talent pipeline, and drive collaborative cyber innovation.

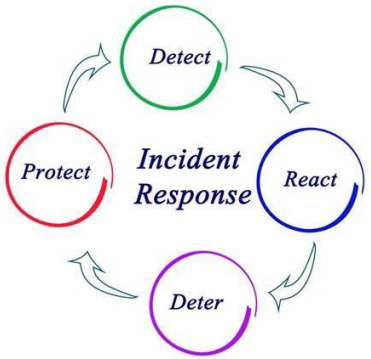
- **San Diego Regional Cyber Lab**
  https://www.sandiego.gov/cyber-lab
  Mission to provide the greater San Diego region with coordinated cybersecurity awareness through collaborative access to tools, intelligence, and a trained and capable workforce.

- **Local Information Security Organization Chapters**
  - Bsides - http://www.securitybsides.com
  - Cloud Security Alliance (CSA) – https://www.meetup.com/Cloud-Security-Alliance-San-Diego
  - IAPP: International Association of Privacy Professionals - https://iapp.org
  - Infragard: Non-profit liaison between the FBI and local community critical infrastructure: https://infragardsd.org/
  - ISACA: Information Systems Audit and Control Association – https://ISACASanDiego.org
  - ISC2: International Information System Security Certification Consortium - https://isc2-san-diego-chapter.org
  - ISSA: Information Security Systems Association – https://www.sdissa.org
  - OWASP:  Open Worldwide Application Security Project - https://owasp.org/www-chapter-san-diego
  - Women in Cybersecurity (WiCys) - https://www.wicys.org/wicys-san-diego

# Resources

There are some aspects of work you need to keep working on and no matter what environment you are in. Continuous learning is very important. It's what I call 'competitive tension', which is about having a competition around. - Viswanathan Anand

## Incident Response Resources




- **FRSecure**
  Same company with the templates. We provide a no cost, no pressure 30-minute consultation in the event of a breach, or you just need a better understanding of what you are experiencing.
  https://frsecure.com/incident

- **ITRC –** Identity Theft Resource Center
  ITRC is a non-profit organization established to minimize risk and mitigate the impact of identity compromise.

- **Your Cyber Insurance Company**
  Your cyber insurance provider should provide you with Incident Response contact information. Make sure you have it **before** something happens.

- **Your Local FBI Field Office**
  If you or your organization is the victim of a network intrusion, data breach, or ransomware attack, contact your nearest FBI field office or report it at tips.fbi.gov.
  https://www.fbi.gov/contact-us/field-offices

- **Internet Crime Complaint Center (IC3)**
  IC3 provides the public with a reliable and convenient reporting mechanism to submit information to the Federal Bureau of Investigation concerning suspected Internet-facilitated criminal activity.
  https://www.ic3.gov

# Thank You!

## Questions?

## Want More Info?

**Joe Erle**
Senior Broker
C3 Insurance

760-688-9131 (direct)
joe@c3insurance.com

www.c3insurance.com

**Dave Tuckman**
Information Security Consultant
FRSecure

dtuckman@FRSecure.com
disacasandiego@gmail.com

www.FRSecure.com