Clare Computer Solutions
Realize the Power of Technology

Omnistruct
Cybersecurity Programs That Work

Six Things You Need To Know About Common Cyber Insurance Underwriter Requirements

An Webinar Series on Cyber Security, Privacy, and Risk for Business Leaders

August 16, 2022

NOTICE: All slides are for Continuing Learning Education Purposes to address Operational management of a solo law office, law firm or corporate law department

Housekeeping

1. *All questions can be entered into the Q&A section of Zoom. (Toolbar Tab: Q&A)*

2. *We have a live Poll that can be taken at any time during the webinar. (Toolbar Tab: Poll)*

3. *Private message Kyle with any concerns, requests, or anonymous questions.*

4. *Our next event will highlight legal impact assessments on privacy, please visit our events page for more event information and to sign up for the next event in this webinar series*

Sign Up Now: clarecomputer.com/events

August 16, 2022

Introduction Omnistruct Speaker

George Usi,

Co-Founder, Omnistruct Inc.

CEO – www.omnistruct.com

Board of Directors - www.securethevillage.org

Co-Chair, California IPv6 Task Force – www.cav6tf.org

- Internet Scientist/Plumber and Researcher
- Career started at NTT/Verio security
- Owned Information Security Audit, Software and Networking Businesses since 2003
- Level 2 Certified Blacksmith
- **Proud Dad of Three Kids and Married to a Lovely Wife**

Key Publications & Accomplishments

- Utility Of Commercial Wireless Study: A Technology Roadmap for Disaster Response for USNORTHCOM; Naval Postgraduate School; Pub 2006

- IPv6 Forum Pioneer Award; Sacramento CA 2007; MetroNet6; Secure Delay Tolerant Communications & First Responder Interoperability research under the mentorship of Jim B0und and Dr Vint Cerf.

August 16, 2022

NOTICE: All slides are for Continuing Learning Education Purposes to address Operational management of a solo law office, law firm or corporate law department

Introduction Clare Computers Speaker

Rod Sweet

Cybersecurity & Cloud Architect,
Clare Computers Solutions

- Working in IT for +40 years for Disney, AT&T, and Sun Microsystems before landing at Clare Computer Solutions.
- In my spare time, I can be found outdoors 4-wheeling Jeep, or taking care of my horses.

Key Publications & Accomplishments

- I helped start what was known as the “1st unified messaging” company in the world, called Blue Silicone.
- In the early 2000s I started my own IT security and consulting business to further my experience.
- Helped Clare Computer Solutions adopt security provisions, and become a security partner for the SF Bay Area.

DISCLAIMER

The information in these slides and presentation are for informational and educational use. The National Institute of Standards and Technologies Privacy Framework (PF), GDPR, CCPA/CPRA, and other data privacy laws are interpreted for educational purposes as part of the public domain and are not intended as audit, consultative, or legal advice from Clare Computers (IT MSP) or Omnistruct Inc (RPO, C3PAO Pending - CYBERab). Speakers are not attorneys or insurance brokers. Any topics covered where regulations, laws, or insurances of any kind are referenced should be reviewed by a licensed attorney or insurance broker respectively.

In terms of safety and security of the Internet... I would have to argue that we are not in a very good place right now.

June 2020 - Dr. Vint Cerf
Co-creator of the Internet, NIST VCAT

Secure The Village Webinar Vint Cerf:
https://youtu.be/PPFeh_105aM?t=433
https://www.nist.gov/director/vcat/biography-dr-vinton-g-cerf

What We Will Cover Today

1

Cyber Risk Introduction, Overview, & Metrics

2

Cyber Insurance Six Things You Need To Know

3

List of Things You Should Be Doing Now

CYBER RISK INTRODUCTION, OVERVIEW, & METRICS

August 16, 2022

NOTICE: All slides are for Continuing Learning Education Purposes to address Operational management of a solo law office, law firm or corporate law department

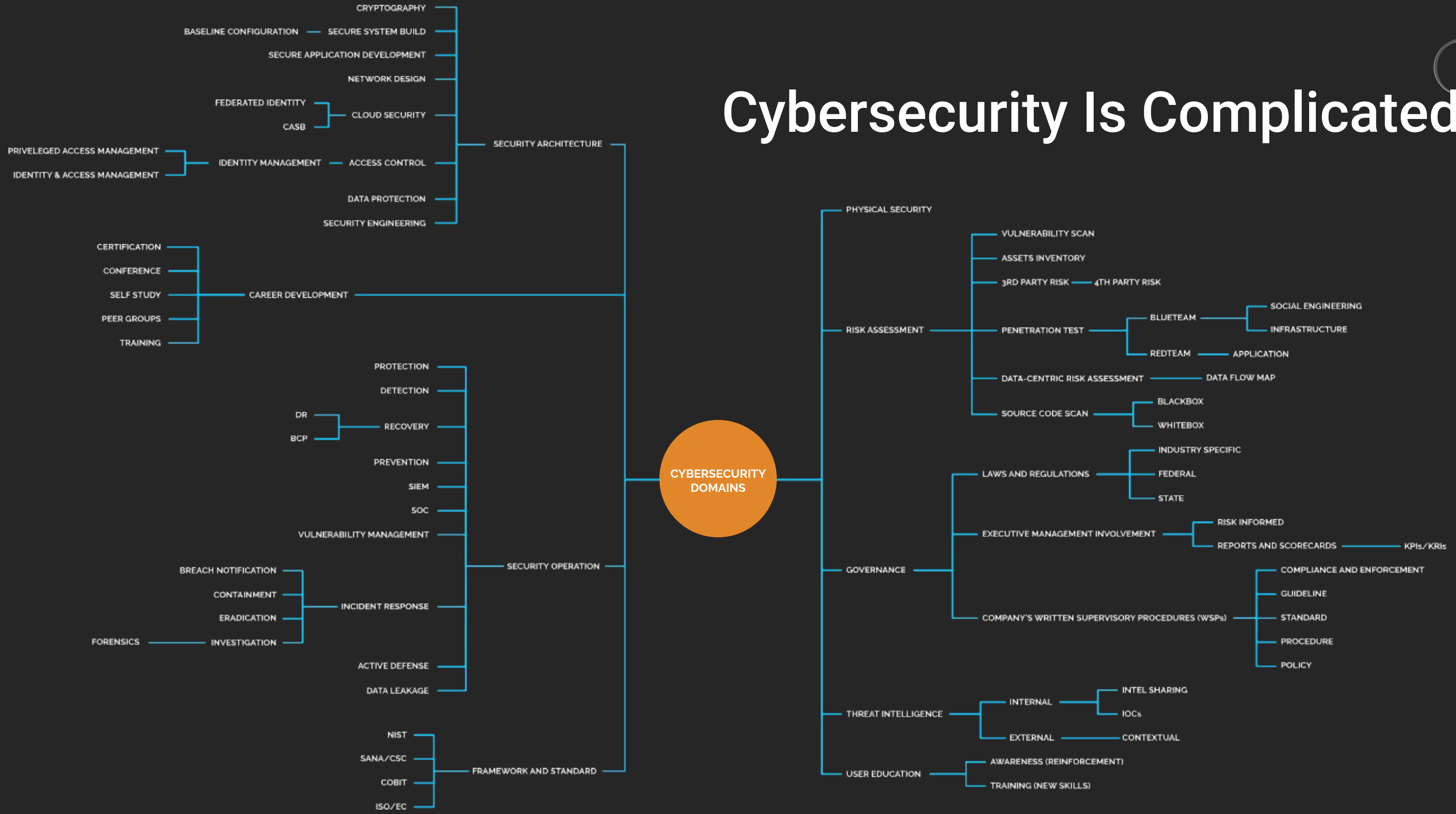
Cyber Risk Airbags Are Lacking

Leaders need a “documented cyber risk airbag” for when regulators, customers, and insurance providers want proof that you are measurably prepared for when hackers succeed.

Compliance 🟧 Worker 🟦

NIST® CSF and PF with cyber-Governance helper/ tools / leaders
What About?.... Policy / Cyber Risk / Departmental / Legal ⬜

Cybersecurity Is Complicated!



- CYBERSECURITY DOMAINS
  - SECURITY ARCHITECTURE
    - CRYPTOGRAPHY
    - SECURE SYSTEM BUILD
      - BASELINE CONFIGURATION
    - SECURE APPLICATION DEVELOPMENT
    - NETWORK DESIGN
    - CLOUD SECURITY
      - FEDERATED IDENTITY
      - CASB
    - ACCESS CONTROL
      - IDENTITY MANAGEMENT
        - PRIVELEGED ACCESS MANAGEMENT
        - IDENTITY & ACCESS MANAGEMENT
    - DATA PROTECTION
    - SECURITY ENGINEERING
  - CAREER DEVELOPMENT
    - CERTIFICATION
    - CONFERENCE
    - SELF STUDY
    - PEER GROUPS
    - TRAINING
  - SECURITY OPERATION
    - PROTECTION
    - DETECTION
    - RECOVERY
      - DR
      - BCP
    - PREVENTION
    - SIEM
    - SOC
    - VULNERABILITY MANAGEMENT
    - INCIDENT RESPONSE
      - BREACH NOTIFICATION
      - CONTAINMENT
      - ERADICATION
      - INVESTIGATION
        - FORENSICS
    - ACTIVE DEFENSE
    - DATA LEAKAGE
  - FRAMEWORK AND STANDARD
    - NIST
    - SANA/CSC
    - COBIT
    - ISO/EC
  - PHYSICAL SECURITY
  - RISK ASSESSMENT
    - VULNERABILITY SCAN
    - ASSETS INVENTORY
    - 3RD PARTY RISK
      - 4TH PARTY RISK
    - PENETRATION TEST
      - BLUETEAM
        - SOCIAL ENGINEERING
        - INFRASTRUCTURE
      - REDTEAM
        - APPLICATION
    - DATA-CENTRIC RISK ASSESSMENT
      - DATA FLOW MAP
    - SOURCE CODE SCAN
      - BLACKBOX
      - WHITEBOX
  - GOVERNANCE
    - LAWS AND REGULATIONS
      - INDUSTRY SPECIFIC
      - FEDERAL
      - STATE
    - EXECUTIVE MANAGEMENT INVOLVEMENT
      - RISK INFORMED
      - REPORTS AND SCORECARDS
        - KPIs/KRIs
    - COMPANY'S WRITTEN SUPERVISORY PROCEDURES (WSPs)
      - COMPLIANCE AND ENFORCEMENT
      - GUIDELINE
      - STANDARD
      - PROCEDURE
      - POLICY
  - THREAT INTELLIGENCE
    - INTERNAL
      - INTEL SHARING
      - IOCs
    - EXTERNAL
      - CONTEXTUAL
  - USER EDUCATION
    - AWARENESS (REINFORCEMENT)
    - TRAINING (NEW SKILLS)

Cybersecurity Without Cyber Risk Management Is Untenable!

Getting Hacked Is A Matter of

“When”

August 16, 2022

NOTICE: All slides are for Continuing Learning Education Purposes to address Operational management of a solo law office, law firm or corporate law department

Leaders Are

Accountable

August 16, 2022

NOTICE: All slides are for Continuing Learning Education Purposes to address Operational management of a solo law office, law firm or corporate law department

A “Make Cyber Risk A Technical Problem” Mindset Is Like

Keeping Food In Your Tent At Camp

August 16, 2022

NOTICE: All slides are for Continuing Learning Education Purposes to address Operational management of a solo law office, law firm or corporate law department

A “Governed Cyber Security, Privacy, & Risk” Mindset is Like

Keeping Food In a Bear-Proof Cooler Away From Your Tent

August 16, 2022

NOTICE: All slides are for Continuing Learning Education Purposes to address Operational management of a solo law office, law firm or corporate law department

Government “Somewhat” To The Rescue

NIST

“Fundamentally, there is no perfect security… if an organization has a solid argument that it has implemented, and maintains safeguards based on the [NIST FRAMEWORKS], there is a much-improved chance of more quickly dispatching litigation claims and allaying the concerns of regulators.”

Burns & Levinson LLP -2018

Source: Legal Intelligence JD Supra: https://www.jdsupra.com/legalnews/the-benefits-of-the-nist-cybersecurity-76753/

NOTICE: All slides are for Continuing Learning Education Purposes to address Operational management of a solo law office, law firm or corporate law department

Cyber Risk Metrics

August 16, 2022

NOTICE: All slides are for Continuing Learning Education Purposes to address Operational management of a solo law office, law firm or corporate law department

Compare: Cybersecurity Ground War & Cyber Risk Air War

What IT Pros have been doing for years “in the trenches” to stop/prevent hackers from succeeding…

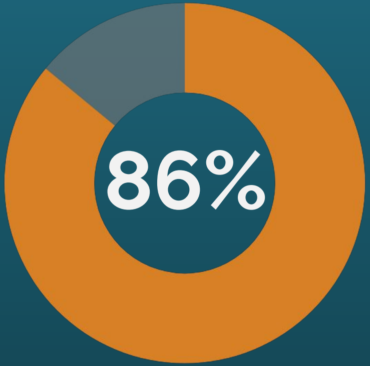
… we are losing the battle

The cyber risk Business & Governance “Blueprint” for security, privacy, and risk;

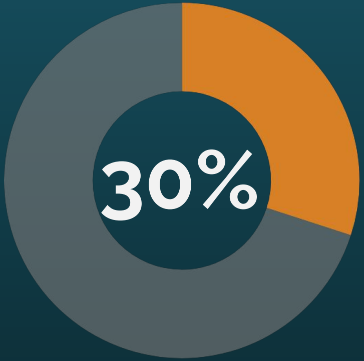
Sanction-driven by regulatory, industrial, and statutory requirements to win the “war”

https://www.inc.com/jeff-barrett/collecting-data-is-all-about-trust-heres-how-to-earn-it.html

A Cyber Risk Gap Exists



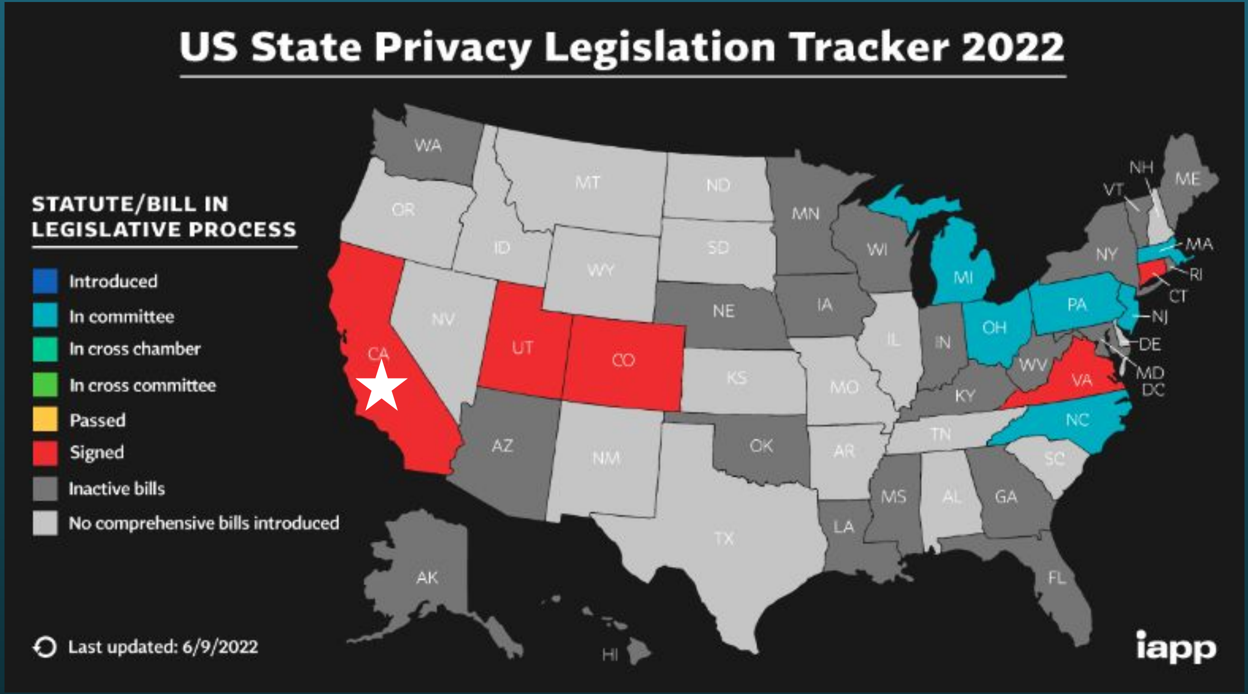
Leadership Comfort Level With Security Risk Management Strategy



Staff Comfort Level With Security Risk Management Strategy

ISACA Reference:
https://www.techrepublic.com/article/report-despite-more-cyberthreats-during-covid-19-most-businesses-confident-about-cybersecurity/

Growing Us Data Privacy Laws By State



★ California Privacy Protection Agency (CPPA) Established to Hire “More Regulatory Bears” That Will Enforce CCPA/CPRA:

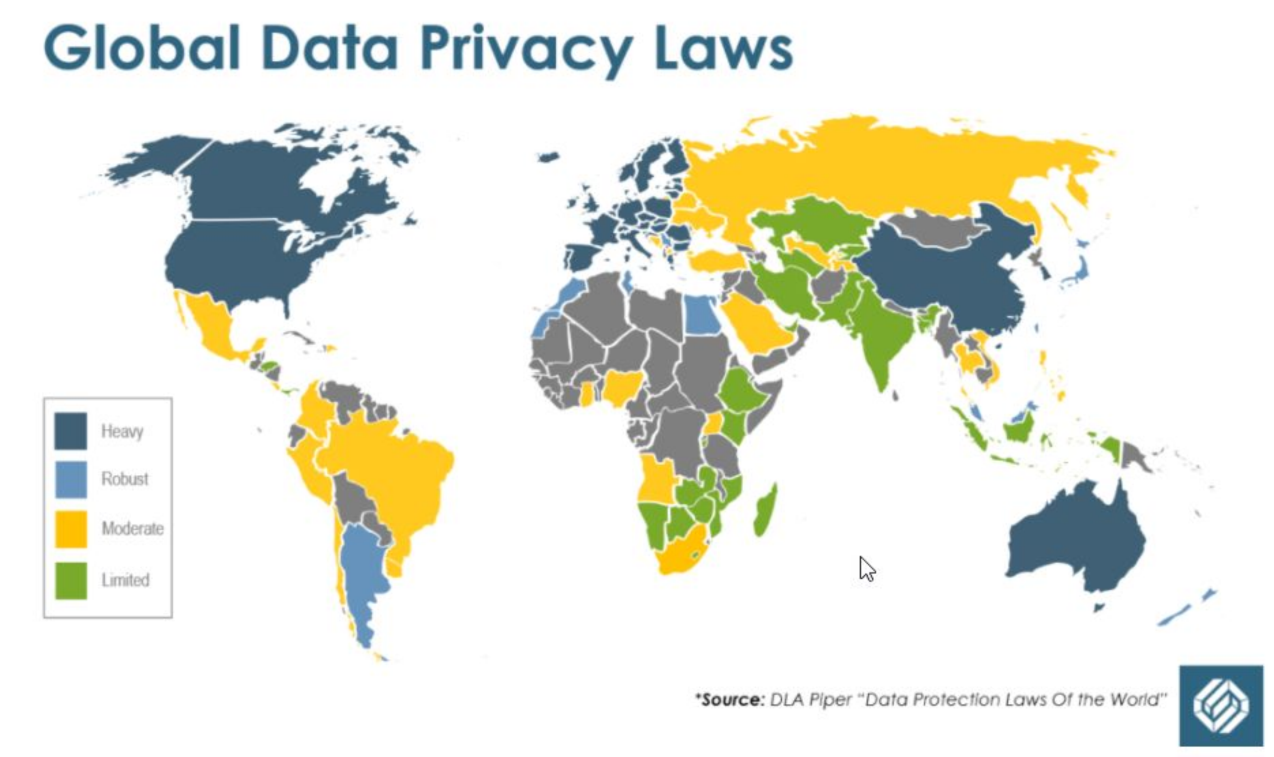
- 1/1/2020 Compliance Req’d
- 1/1/2021 Voters reinforced
- 1/1/2023 HR/Employees

https://termly.io/resources/articles/privacy-laws-in-the-us/#data-privacy-laws-by-state
Map Credit IAPP®: https://iapp.org/resources/article/us-state-privacy-legislation-tracker/

International Data Privacy Laws

KEY COUNTRIES TO NOTE:

European Union -	GDPR
UK (Brexit Note) -	DPA
Australia –	APP/PA
Brazil -	LGPD
Canada -	PIPEDA
China -	PIPL
Hong Kong –	PDPO S1
Singapore -	PDPA
South Korea -	PIPA
Turkey -	PDPL


Global Data Privacy Laws

*Source: DLA Piper "Data Protection Laws Of the World"

"Key Countries to Note" Credit IAPP®: https://iapp.org/media/pdf/resource_center/global_comprehensive_privacy_law_mapping.pdf

August 16, 2022

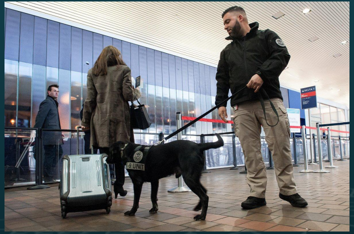
NOTICE: All slides are for Continuing Learning Education Purposes to address Operational management of a solo law office, law firm or corporate law department

Digital “K9” Cyber Insurance Inclusions Looming

Firewall & Anti-Malware

*Showing up in ransomware insurance renewals now!

EndPoint Detection/Response



*Cyber Risk Management with SOC/SIEM

https://www.computerweekly.com/feature/Cyber-insurance-What-does-a-CISO-need-to-know

August 16, 2022

List of Top Cyber Threats Where Sanctions Are Likely

1. Data breach of highly confidential information in any way (digitally or physically)

2. Ransomware software that absconds with data and freezes you out of your computer (81% of all breaches in 2021)

3. Phishing by sending a questionable message or equest in hopes confidential information can be taken *(*note: hackers are targeting law firms with ransomware attacks)*.

* https://www.forbes.com/sites/forbestechcouncil/2021/03/12/ransomware-attackers-take-aim-at-law-firms/
* https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-mandatory-cybersecurity-cle-credits-at-a-bar-near-you

EVERYONE SHOULD PREPARE FOR “WHEN” HACKERS SUCCEED

> “*NIST must disseminate, and publish on its website, standard and method resources that small business may use voluntarily to help identify, assess, manage, and reduce their cybersecurity risks*”

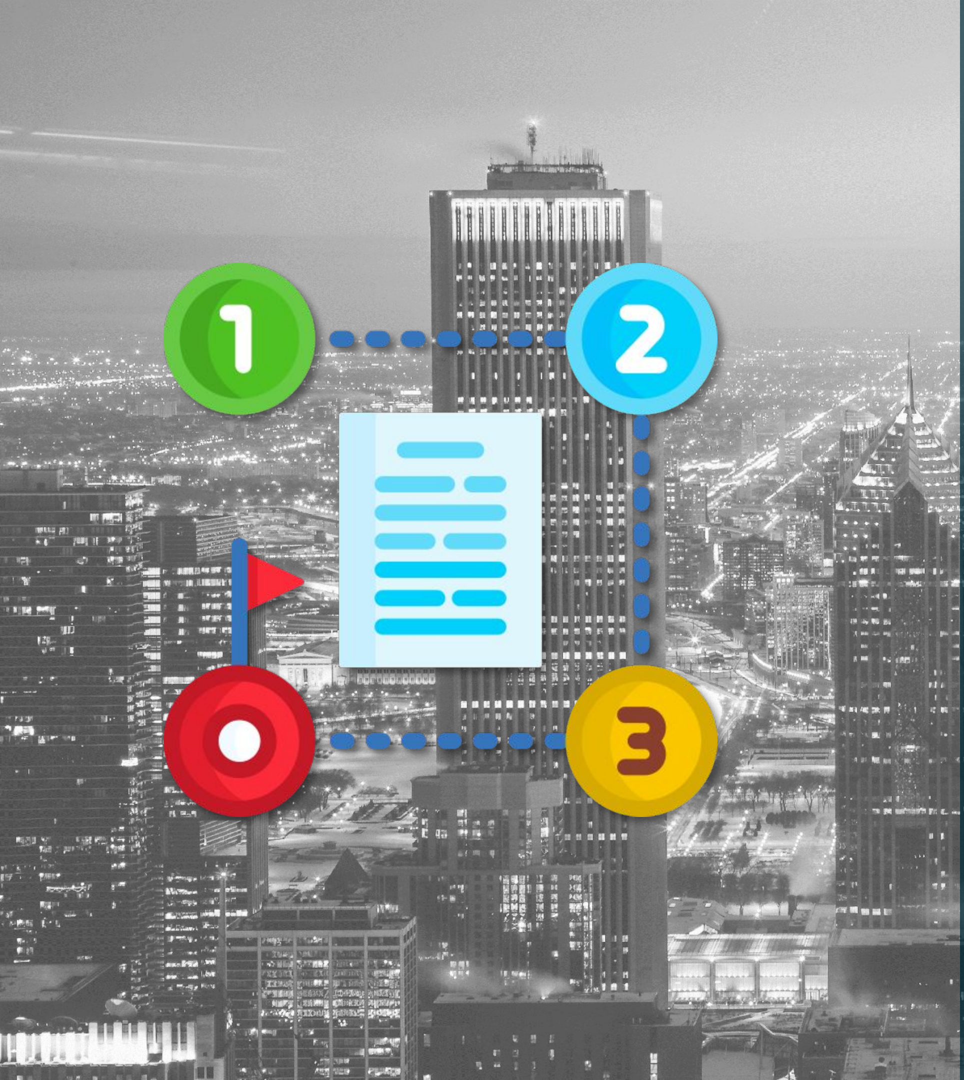
- NIST Small Business Cybersecurity Act of 2018

https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-is-strengthening-americas-cybersecurity/

Cyber Insurance Six Things You Need To Know

August 16, 2022

NOTICE: All slides are for Continuing Learning Education Purposes to address Operational management of a solo law office, law firm or corporate law department

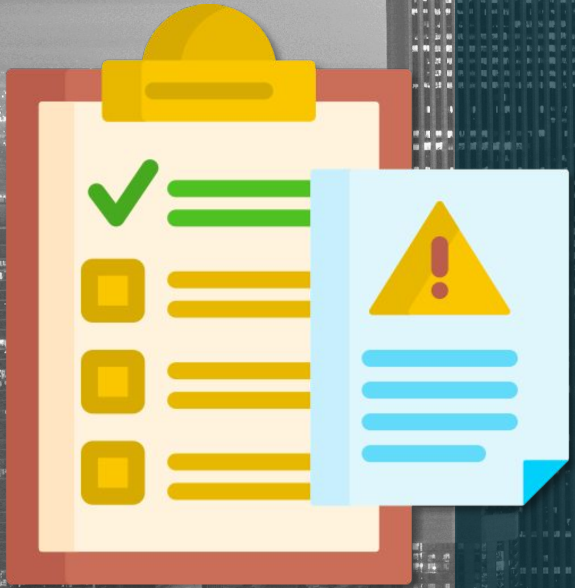


1. Close Unused Remote Desktop Protocol Ports

Remote Desktops Protocol allows the remote workforce to access office desktops and company databases from afar.

- ***Close all unused RDP ports***
- ***Protect all ports being used***
  - ***VPN***
  - ***Multifactor Authentication (MFA)***

It's these RDP ports that are major vulnerabilities. With over 50% of ransomware attacks utilizing this attack vector, closing these is necessary for businesses today.



2. Use Multifactor Authentication (MFA)

Complex passwords don’t provide enough security to protect business data. This means, another layer of security has become the standard to authenticate users. In many cases, authentication is a fingerprint, unique code, or applications.

Multifactor Authentication (MFA) is used to secure personal information, passwords, or general access, by stopping brute-force attacks where criminals automate rapid attempts to try multiple usernames and passwords to break into the system.

When these attacks occur, their goal is to steal information that is then sold on the dark web. When sold, this information is typically used to access financial or administrator accounts with greater success.

For that reason, many cyber underwriters love seeing a business actively already using MFA for all email accounts and key business software.

3. Data Management Strategy

Your data management strategy can reduce the likelihood of a catastrophic loss. By using cloud services, it’s important to ensure the use of authorized access controls.

This allows businesses to:

- ***Better control security checkpoints***
- ***Audit third-party vendor authorization***
- ***Avoid catastrophic data loss***

Cyber-insurance underwriters like when a company’s data is stored and segregated properly. Ideally, splitting client records for example across multiple servers, to prevent complete compromise and data loss.

4. Run Endpoint Detection and Response

Cyber insurance underwriters continue to advise businesses that firewalls and antivirus are no-longer enough.

Endpoint Detection and Response (EDR) tools monitor devices connected to the network to make sure they are secure and have not been compromised. This is critical, as employees can use devices that become compromised by malicious links, can unleash attacks on company networks.

Remember:
An endpoint is anything from an employee workstation, laptop, tablet, server, or cellphone.

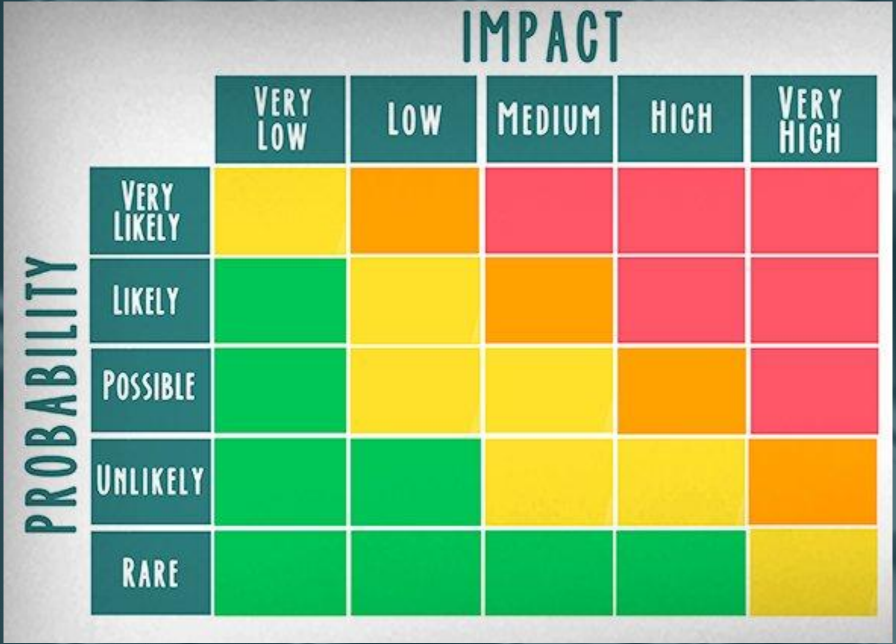
5. Segment Backup Data From the Main Network

Backups can do more than just back up records, what is most important is how this data is handled, what is done with that backup information after. In most cases, companies are backing-up servers, but what good will that do if the server fails, and you’ve stored these backups on it?

Insurance underwriters prefer seeing backup data remain separated across multiple servers or stored offline in an off-site location. If something needs to be recovered, you have a secured reference-point to recover from.

6. Make risk management a priority!

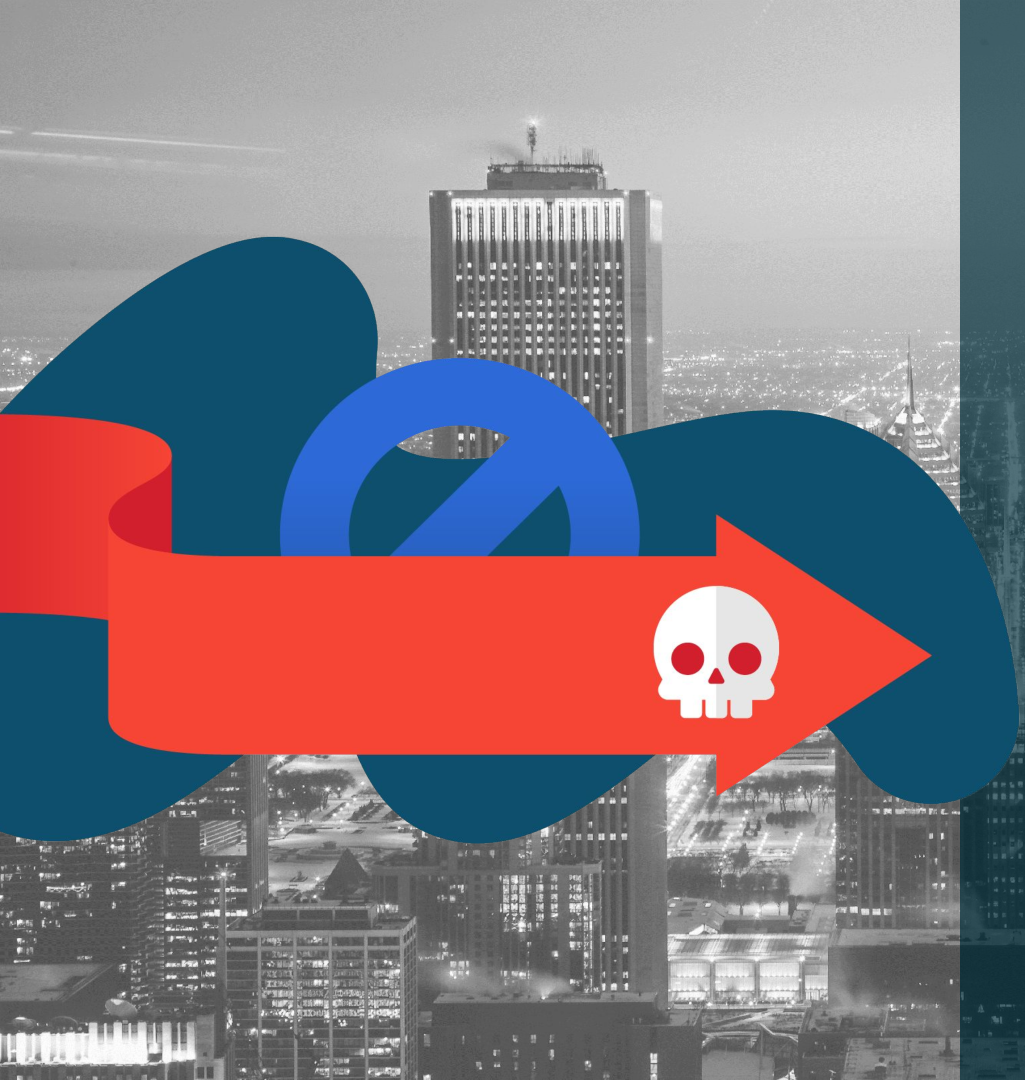
1) Identify the risks
2) Measure the probability
3) Assess the impact
4) Calculate the total risk
5) Update the matrix with the team



IMPACT

PROBABILITY

	Very Low	Low	Medium	High	Very High
Very Likely	🟨	🟧	🟥	🟥	🟥
Likely	🟩	🟨	🟧	🟥	🟥
Possible	🟩	🟨	🟨	🟧	🟥
Unlikely	🟩	🟩	🟨	🟨	🟧
Rare	🟩	🟩	🟩	🟩	🟨



Cyber Insurance Underwriters Will Also Look at the Following:

1. Any policies and procedures you have in place in terms of cyber risk management. *(Etc. Computer Use Policy, Internet Use Policy. Email Use Policy)*
2. If you have a designated staff member in charge of these policies.
3. The designated staff members must know about the different kinds of data you are storing, and how it is being stored.
4. SOC/SIEM & EDR for ransomware

List of Things You Should Be Doing Now

August 16, 2022

NOTICE: All slides are for Continuing Learning Education Purposes to address Operational management of a solo law office, law firm or corporate law department

What Should You Do First?

1

Talk to Your Clare vCIO about additional Cyber Risk Education

ⓘ

Clare is a NIST-attested Managed Service Provider.

What Should You Do Second?

2

Strengthen Ground War

ⓘ

Make sure all your technology suppliers have their own security program that follows US guidelines built by NIST or equivalent.

What Else Should I Do?

3

Strengthen Your “Air War”

ℹ

Using a certified NIST expert and auditor (like Omnistruct) may provide Safe-Harbor from sanctions if you are hacked.

Ground War Do's – General List

Here Are Items Suggested

1 – Use Endpoint Detection & Response technology
2 – Use multi-factor authentication with strong passwords
3 – Invest in a password manager
4 – Use VPNs when traveling to encrypt your data when using wifi
5 – Encrypt sensitive data

Easy Button: Talk to Clare Computers about IT Managed Services

https://www.legalreader.com/how-law-firms-can-strengthen-their-cybersecurity/

Ground War Do's - Cyber Insurance List

Here Are What Cyber Insurance Underwriters Generally Expect You Be Doing Continuously For Your "Ground War" Before Underwriting a Cyber Insurance Policy:

1 – Block ports for "remoting" into office computers
2 – Use multi-factor authentication
3 – Refresh all "End of Life" tech
4 – Use endpoint detection and response
5 – Backups of critical data– 3-2-1
6 – Add SOC/SIEM Service
7 – Educate Leaders on Cyber Risk Management ✔

Easy Button: Talk to Your Clare Computers vCIO

https://www.northbaybusinessjournal.com/article/industrynews/6-risks-cyber-insurance-underwriters-look-for-in-your-business-data-securit/

Air War Do’s – Basic Cyber Governance

These are leadership/owner items to consider
Cyber Insurers also want to see cyber risk management prioritized. The best way to do that is to

1 – Cyber security awareness program & training for everyone
2 – Have written security policies in place and demonstrate enforcement
3 – Use/affirm service providers attested to US guideline in cyber; NIST
4 – Establish a cybersecurity “team” and meet at least quarterly
5 – Create an incident response plan with network and data map
6 – Customize Training for sensitive data handlers (ie: HR, B2C Marketer)
7 – Add Cyber Risk Posture Metrics to Quarterly Business/Board Reviews

Easy Button: Talk to your Clare vCIO about a cyber governance readiness assessment

https://www.northbaybusinessjournal.com/article/industrynews/6-risks-cyber-insurance-underwriters-look-for-in-your-business-data-securit/

NOTICE: All slides are for Continuing Learning Education Purposes to address Operational management of a solo law office, law firm or corporate law department

Air War Do's – Advanced Cyber Governance Data Protect

For Those of Unable to Avoid Stewardship of Personal Information, especially when marketing, consider these five actions:

1 – Review existing personal data collected and decide what is required for business purposes
2 – Define and document the business purpose of data collection
3 – *MARKETING* - Update privacy policies (if wordpress driven, require your marketer to add wordplus Compliance plugin);
4 – Monitor quarterly and revise appropriately with record of what is done and why
5 – Be prepared to invest in Data Subject Access Requests
6 – Establish a NIST CSF Written Information Security Program
7 – Establish a NIST PF Written Privacy Program

Easy Button: Talk to your Clare vCIO about NIST-attested cyber governance readiness & legal regulatory impact assessments

https://www.northbaybusinessjournal.com/article/industrynews/6-risks-cyber-insurance-underwriters-look-for-in-your-business-data-securit/

Critical “Do & Don’t” Actions

DO:

1. Understand what data privacy laws you must comply with;
2. Transfer out the cyber risk of being a collector of personal information;
3. Make sure privacy policies are posted on every site/app main page.

DON’T:

1. Collect personal information in your hosted Wordpress or CMS forms;
2. Collect personal information without applicable privacy rights notice;
3. Retain unnecessary personal information on paper.

What You Need To Be Doing Now

1 Conduct Secure Risk Assessment

2 Get Key Leader Buy In For Cyber Security Program Governance

3 Address Ground War Items

4 Address Air War Items

5 Start Auditing 3rd Parties

August 16, 2022

NOTICE: All slides are for Continuing Learning Education Purposes to address Operational management of a solo law office, law firm or corporate law department