Cybersecurity Risks and Considerations: Threats and Solutions for the Construction Industry

Minnesota AGC Summit

January 17-18, 2023

faegre drinker

Presented by:

Kenneth K. Dort
Partner
Intellectual Property
Chicago
+1 312 569 1458

1

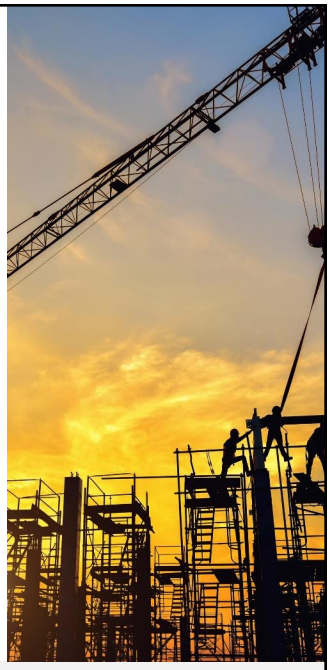
Overview

- Construction Landscape
- Concerns/Threats/Vulnerabilities
- Trends
- Strategies
- Best Practices
- Questions/Discussion

2

Factors of Vulnerability

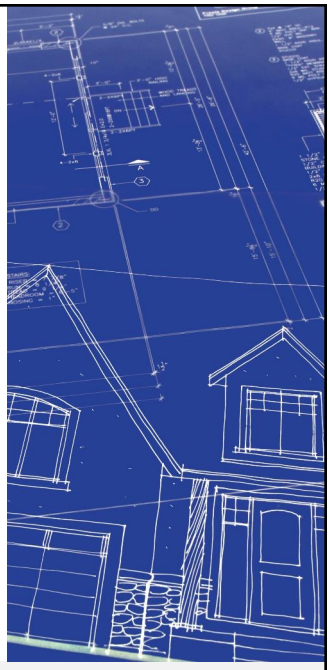
- Lack of Regulation
  - Industry has not prioritized implementing cybersecurity measures into their business models
    - IBM Ponemon study found that 74% of construction-related organizations are not prepared for a cyberattacks and have not formed or implemented a cybersecurity response plan
    - Being slow to implement cybersecurity measures has made it an attractive target for threat actors
- Construction 4.0
  - Industry has begun to adopt new technologies which has greatly increased exposure to remote cyber attacks
  - Construction industry has increased its usage of AI, IOT and robotics, which require added security controls and privacy risk assessments; they are also vulnerable to cyber attacks and when paired with lack of preparedness, create an attractive target for threat actors



3

Factors of Vulnerability II

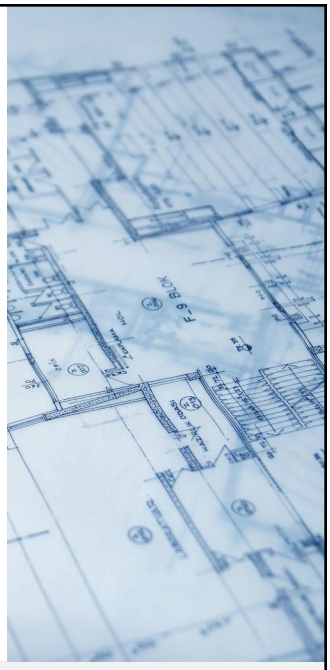
- Nature of data stored by construction companies
  - Construction firms store large amounts of sensitive business data and personal information, making them lucrative targets for cybercriminals. If this data is improperly accessed, it may result in reputational damage, regulatory fines and related lawsuits
  - Confidential and proprietary info is digitally stored and shared across projects and their long information technology chains
  - Construction transactions contain significant amounts of personal information and sensitive business data, particularly regarding financial data, which entices threat actors
- Elevated third-party exposures
  - Construction companies frequently work with multiple vendors or third-party contractors, increasing their cyber exposure. After all, a data breach within any one of these partnered companies could result in widespread cyber losses
  - As noted above, much confidential and proprietary info is digitally stored and shared across projects and their long information technology chains
  - Construction companies work with a variety of vendors, and each transaction may involve several parties, providing ample opportunity for an internal or external bad actor to wreak havoc



4

Types of Attacks

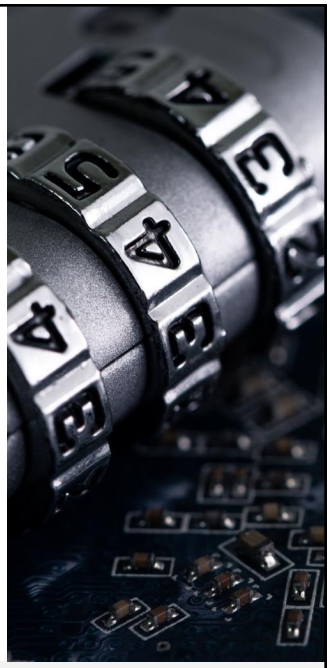
- Ransomware
  - Ransomware, or when a threat actor holds a computer system hostage for payment, can limit a construction company's access to critical systems and potential delay work at Project. Moreover, a construction company may be left with little choice but to incur the financial responsibility of paying the ransom. However, damage from a ransomware event is not simply limited to the payment of the ransom but may also include reputational damage
- Fraudulent wire transfers
  - Fraudulent wire transfers, often the result of social engineering, present a substantial risk the construction industry, who are often moving large sums of capital around. Falling victim to fraudulent wire transfer not only presents dire fiscal issues for a construction company but can also lead to server reputation harm



5

Types of Attacks II

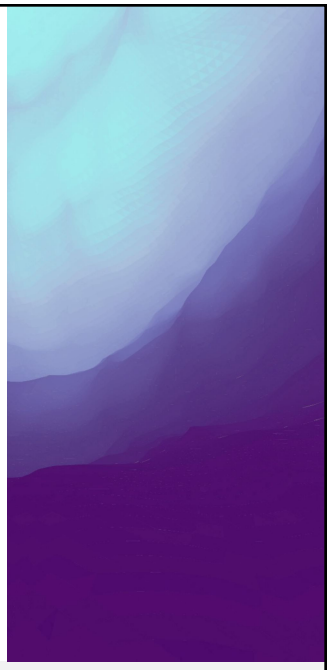
- Breach/theft of IP
  - If a construction company is holding highly sensitive blueprints or schematics in its computer system, breach of these computer systems could result in major reputational damage and potential lawsuits.
- Downtime or business interruptions
  - The construction industry is heavily reliant on the ability to deliver projects on a deadline. A cyber-attack on a construction company's software or equipment could potentially cause a delay in the project while the cyber-attack is properly addressed



6

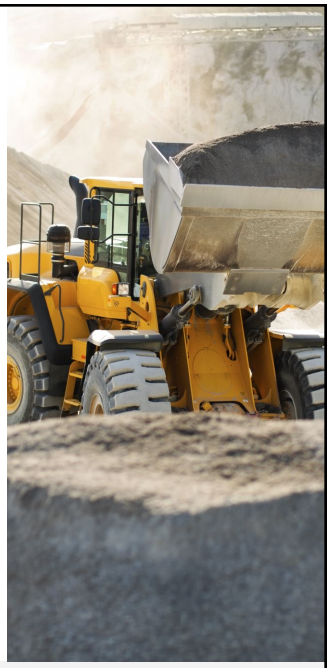
Attack Vectors

- 3D Building Information Modeling (“BIM”)
  - Builds information models use computer-based files used to support efficient decision-making for planning, design, construction, and building operations and maintenance.
- 5D BIM
  - Provides an enhanced visualization and project-management platform. In the future, augmented- and virtual-reality technology will be added to allow offices and the worksite to collaborate in real-time
- Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition Systems (SCADA)
  - Monitors and controls equipment and plant operations
- Drones
  - Enables job site surveillance, surveying and access to previously inaccessible places



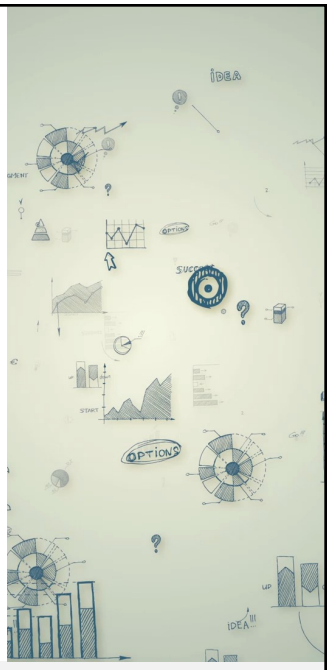
Attack Vectors II

- Autonomous Construction Machinery
  - Used for the remote navigation of excavators, bulldozers, backhoes and dump trucks for higher utilization rates and lower operator costs
- Robotics
  - The deployment of robotics in bricklaying and road paving, to replace highly repetitive, systematic manual processes
- Biometrics
  - Increasingly used to manage and control construction sites and projects, through access control to secure sites, on-site attendance reporting, health and safety, compliance, and remote management of multiple workforces



Attack Vectors III

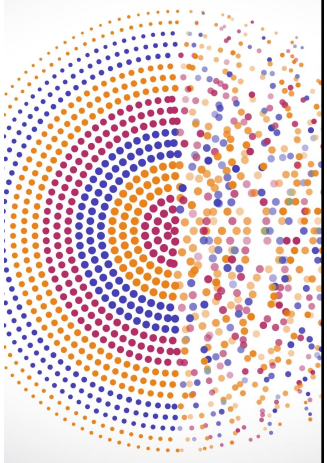
- Cloud technology
  - The use of vendors to store data on behalf of the business
- Mobile devices
  - Allows the highly decentralized construction industry to enhance collaboration at all stages of the construction process, including productivity tracking, report generation, document management, material logistics, inventory management and data analytics.
- Internet of Things (IoT)
  - Provides for remote operation of wearables and machinery, supply replenishment, tracking of tools and equipment and remote usage monitoring



9

Trends – Construction Cyber Threats

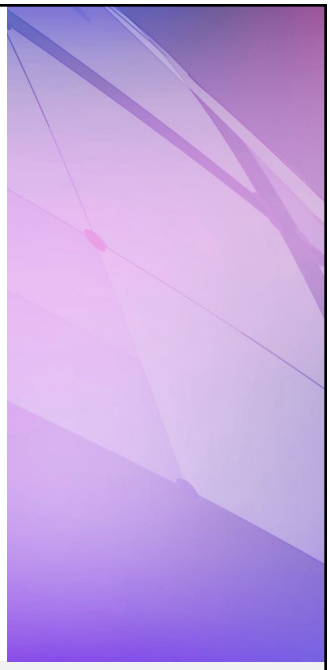
- Projected that cybercrime will cost businesses approximately $6 trillion per year on average through 2021
- In 2021, ransomware cost businesses more than $29 billion in damages; a study by Safety Detectives found that construction was the third most common industry to experience ransomware attacks in 2021 (13.2 percent of total ransomware attacks in North America)
  - Another study found that construction was the top industry targeted by ransomware in 2021
- Advisen data shows cyber losses in the construction industry have risen since 2010, with the most dramatic increase occurring in 2020



10

Trends – Construction Cyber Threats II

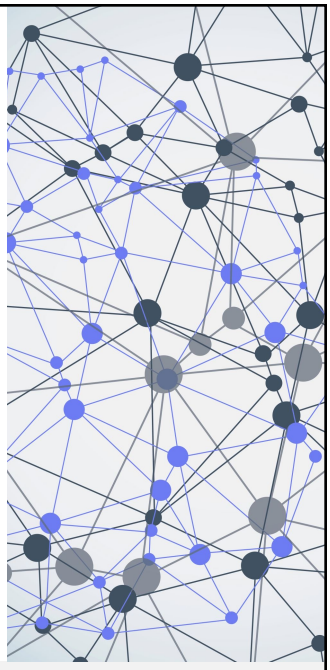
- Unauthorized contact or disclosure is the most common type of cyber loss in construction, accounting for 44% of recorded losses
  - These losses include any event in which information is exposed to unauthorized parties
- Malicious data breaches and ransomware attacks account for 30% and 10% of the remaining cyber losses, respectively
- Ransomware attacks thus represent the third-most frequent type of cyber loss in construction
- Cyberattacks in the construction industry most frequently originate from attacks on company servers, according to Advisen data



11

Trends – Construction Cyber Threats III

- Telephone communications and emails are the second- and third-most frequent sources of cyber losses in the construction industry
- Personal identifiable information (e.g., names, Social Security numbers and driver's license numbers) are targeted in 60% of cyberattacks in the construction sector
- Personal financial information and personal health information are targeted in 36% and 4% of cyberattacks in the industry, respectively
- Between 2017-2018 a Forrester survey revealed that more than 75% of respondents in the construction, engineering, and infrastructure industries had experienced a cyber incident



12

Ransomware

13

Ransomware

- Ransomware is a type of malicious software, or malware, that encrypts data on a computer making it unusable
- A malicious cyber criminal holds the data hostage until the ransom is paid
- If the ransom is not paid, the victim's data remains unavailable
- Cyber criminals may also pressure victims to pay the ransom by threatening to destroy the victim's data or to release it to the public
- Although cyber criminals use a variety of techniques to infect victims with ransomware, the most common means of infection are email phishing campaigns, Remote Desktop Protocol (RDP) vulnerabilities and software vulnerabilities

14

Ransomware (con'd)

- Cyber actors hold systems or data hostage until a ransom is paid for a decryption key
- Cyber actors also threaten to publish exfiltrated data or sell it on the dark web
- Increasingly, cyber actors request virtual currency transfers as a ransom payment method
- In some cases, a decryption key was not provided in return to a paid ransom
- In other cases, additional ransom was demanded

Source: United States Secret Service, Cybercrime Investigations, Preparing for a Cyber Incident – A Guide to Ransomware at https://www.secretservice.gov/sites/default/files/reports/2020-12/Preparing%20for%20a%20Cyber%20Incident%20-%20A%20Guide%20to%20Ransomware%20v%201.0.pdf

15

Ransomware Trends – 2022/2023

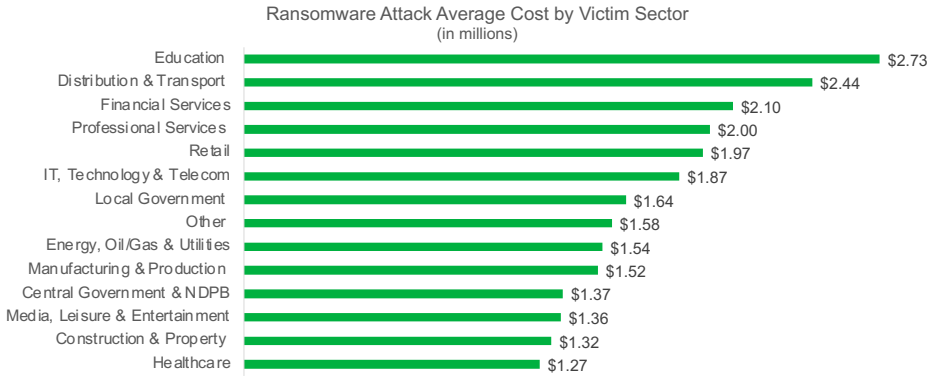
- Initial Access Brokers
- Ransomware-as-a-Service
- Double Extortion – Encryption Keys and Exfiltration
- Malicious Cloud SaaS Apps
- Attacks on Critical Services – Infrastructure, Governments

16

RANSOMWARE 2021 TRENDS

Ransomware impacts & costs

- Globally, and including downtime, network repairs, lost opportunity, and the ransom paid, the average ransomware incident in 2021 has cost **$1.85 million USD**.



17

17

RANSOMWARE 2021 TRENDS

Victim Response Trends

- In 2021, the likelihood that a victim organization chooses to pay a ransom in order to regain access to its data has increased.

2020	2021	
26%	32%	Paid ransom to get data back
56%	57%	Used backups to get data back
12%	8%	Used other means to get data back
94%	96%	Total that got data back

[Image Source: Sophos]

18

18

The Growth and Destruction of Ransomware Attacks is Growing

- There have been thousands of ransomware attacks in 2021 already, but here are the biggest 10 that have had dramatic affects on the power of the ransomware gangs based on their success:
  1. Colonial Pipeline
  2. Brenntag
  3. Acer
  4. JBS Foods (editors note: firm client – just an fyi)
  5. Quanta
  6. National Basketball Association
  7. AXA
  8. CNA
  9. CD Projekt
  10. KIA Motor

19

The Growth and Destruction of Ransomware Attacks Continues

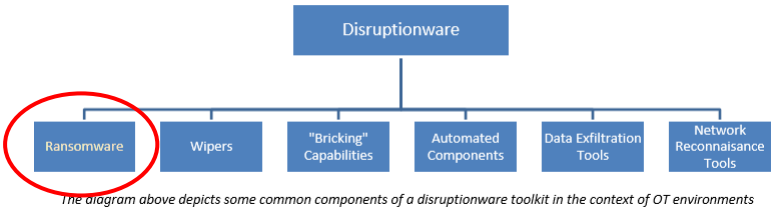
- There have been thousands of ransomware attacks in 2022, but here are 10 of the biggest that have had dramatic affects on the power of the ransomware gangs based on their success:
  1. Bernalillo County, NM
  2. Puma
  3. Government of Costa Rica
  4. Government of Montenegro
  5. Bridgestone
  6. Nvidia
  7. Okta
  8. Puma
  9. Austin Peay State University
  10. City of Wheat Ridge

20

Ransomware is the Bully of the "Disruptionware" family

- Disruptionware is a new and dangerous type of cyberattack
  - Disruptionware has many types of cyberattack possibilities
  - There are multiple tools available to a cyber threat actor implementing a disruptionware attack

Typical Components in Disruptionware

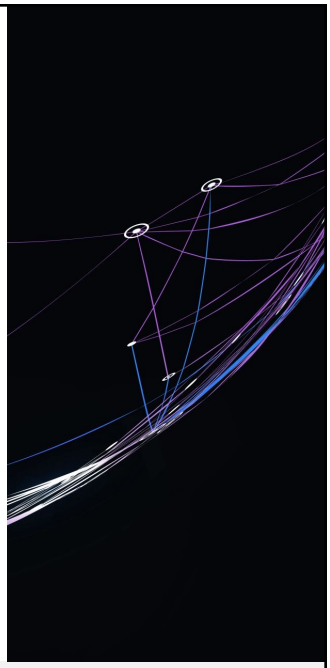


The diagram above depicts some common components of a disruptionware toolkit in the context of OT environments

21

Disruptionware is Growing – and Spreading

- Ransomware is the most common disruptionware attack especially when the goal is financial
- Ransomware is a type of malware or software designed to block access to a computer system or network until a ransom is paid to the cyber threat actors
- Ransomware is dual purpose – if ransom is not paid, attack can also shut down both "IT" and "OT" networks
  - Ransomware cyber threat actors also steal data and threaten to expose it unless ransom paid – on top of the encrypting of a victim's data



22

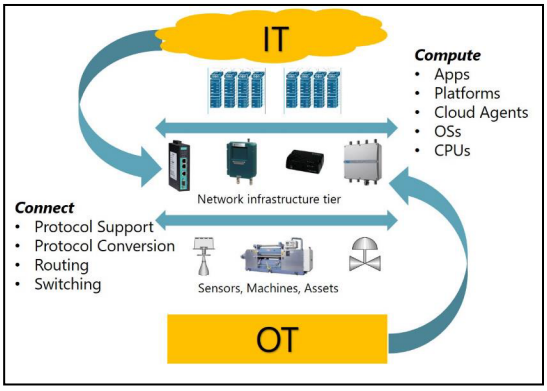
Ransomware Attacks The CIA Triad

- What is the CIA Triad and why is it important?
  - It is the foundation of the basis for Ransomware attacks
  - The CIA Triad is designed to guide policies for information security within an organization:
    - Confidentiality -- helps limit access to information; designed to keep information limited to only those who are supposed to have access
    - Integrity -- assures that the information provided is trustworthy and accurate; ensures that you are looking at the data in an unaltered form
    - Availability -- guarantees reliable access to the information in question by authorized people; ensures those without a need to know do not access information

23

How Does Disruptionware/Ransomware Work?

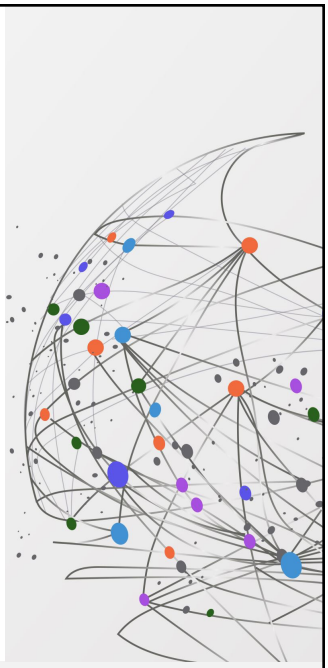
- Disruptionware attacks – through the use of ransomware - focus on **TWO** different victim networks; they usually attack one or both networks in a coordinated effort to create maximum effect
  - **The "IT" or Informational Technology networks** – traditional internal victim company network that we are all familiar with; AND
  - **The "OT" or Operational Technology networks** – OT networks support physical infrastructure, including manufacturing controls, utilities and building management systems (i.e., lights, cooling systems and elevators)



24

What is Disruptionware and how does Ransomware make it work?

- How do the disruptionware/ransomware threat actors institute their battle plan?
  - Many reasonably talented cyber threat actors already know how to attack traditional IT networks – these are more traditional cyberattacks – stealing information and selling it
  - Disruptionware/ransomware threat actors also know how to effectively attack the OT networks – focusing their attacks on critical infrastructure in government, schools, universities and health care industries
  - Disruptionware/ransomware attacks are also growing against the American energy industry – which is, for the most part, not well-prepared to defend itself
  - Disruptionware/ransomware attacks are targeting the growing (and merging) of IT and OT networks; This is used to shut down the victim's Industrial Control Systems (ICS) as a means to extort money



25

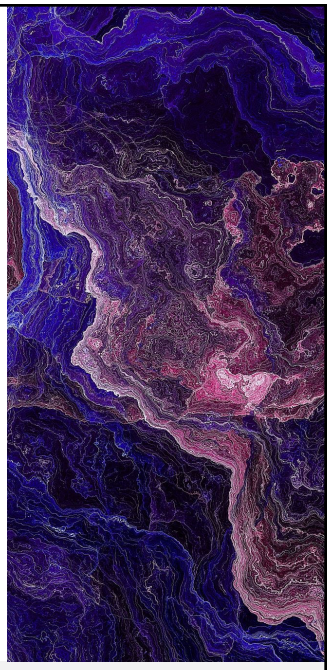
The Spread of Disruptionware

- Malicious cyber threat actors have initially focused their disruptionware and ransomware attacks against several industries, including:
  - Health Care
  - Government
  - Education
  - Energy & Related Infrastructure
- Recently we have seen an evolution of disruptionware
  - In February 2021 there was an attack against a Florida water treatment facility
  - Instead of a demand for money, this threat actor tried to poison the community's water supply by taking over the plant's OT network
  - Many parts of the U.S. infrastructure grid were designed and built with few cybersecurity controls in place, making them very vulnerable to cyberattack
    - **Are these threat actors or foreign nation states?**
- The Florida water treatment attack may be the beginning of an evolution of disruptionware and ransomware attacks against U.S. infrastructure facilities
  - The threat actor did not use ransomware to encrypt either the IT or the OT network
  - The threat actor used their attack to take control of the plant's OT network and access the plant's industrial control system to poison the water supply
  - This could have been a mass casualty event had it not been detected

26

The Spread of Disruptionware/Ransomware

- There have been recent disruptionware/ransomware attacks that have led to patient deaths in both German and American hospitals
  - These deaths were caused by threat actors, using ransomware and inadvertently encrypting the hospitals' OT networks (the networks that were supporting the hospital infrastructure) causing the medical facilities to lose access to and control of portions of their facilities
- Malicious threat actors can use ransomware attacks to fulfill many different needs:
  - Financial gain
  - Personal animosity
  - Political ideology
  - Religious dogma



The Federal Government Tightening Down

- Recently, the Feds have instituted more aggressive cyber-security controls in an attempt to stem the flow of these many ransomware attack
- This includes new regulations and statutes such as:
  - Department of Labor Best Practices for ERISA organizations
  - Department of Homeland Security Mandatory reporting guidelines for pipeline attacks
  - Requiring more federal agencies and requesting private sector entities to expand MFA
  - Far greater information sharing among federal agencies including threat sharing among law enforcement agencies
  - New Internet of Things Cyber Security Act
  - Implementation of the new CMMC for the DOD

Most Frequent Phishing Subject Lines "In-the-Wild"

- Changes to your Health Benefits
- Security Alert: New or Unusual Twitter Login
- Amazon: Action Required – Your Prime Membership has been declined
- Zoom: Scheduled Meeting Error
- Stimulus Cancellation Request Approved

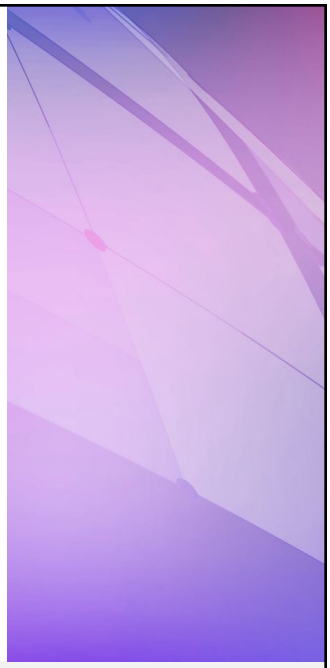
Source: Tessian

29

FBI Statistics -- 2020

- Ransomware by Victim Count: **2,474**
- Ransomware by Victim Loss: ***$29,157,405**
- *Regarding ransomware adjusted losses, this number does not include estimates of lost business, time, wages, files, or equipment, or any third-party remediation services acquired by a victim. In some cases, victims do not report any loss amount to the FBI, thereby creating an artificially low overall ransomware loss rate. Lastly, the number only represents what victims report to the FBI via the IC3 and does not account for victim direct reporting to FBI field offices/agents.

Source: FBI, Internet Crime Complaint Center 2020 Internet Crime Report at https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

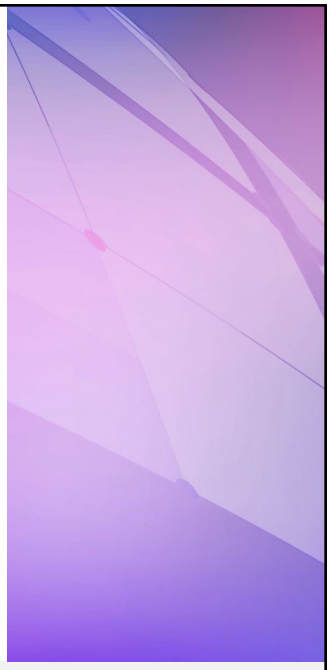


30

FBI Statistics -- 2021

- Ransomware by Victim Count: **3,729**
- Ransomware by Victim Loss: ***$49.2 million**
- *Regarding ransomware adjusted losses, this number does not include estimates of lost business, time, wages, files, or equipment, or any third-party remediation services acquired by a victim. In some cases, victims do not report any loss amount to the FBI, thereby creating an artificially low overall ransomware loss rate. Lastly, the number only represents what victims report to the FBI via the IC3 and does not account for victim direct reporting to FBI field offices/agents.

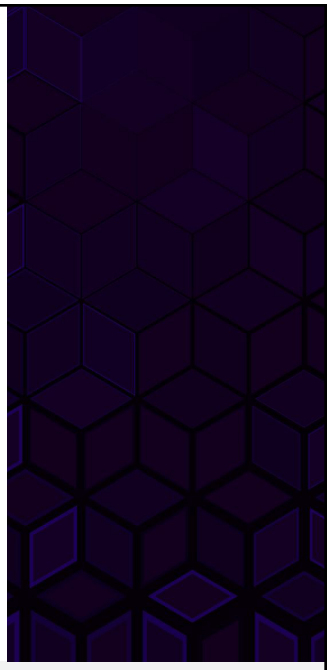
Source: FBI, Internet Crime Complaint Center 2021 Internet Crime Report at https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf



31

White House June 2, 2021 Ransomware Memo to Private Sector

- What We Urge You to Do Now to Protect Against the Threat of Ransomware:
- Implement best practices from President Biden's Improving the Nation's Cybersecurity Executive Order:
  - multifactor authentication (because passwords alone are routinely compromised)
  - endpoint detection and response (to hunt for malicious activity on a network and block it)
  - encryption (so if data is stolen, it is unusable)
  - skilled, empowered security team (to patch rapidly and share and incorporate threat information in your defenses)
- Backup your data, system images and configurations, regularly test them and keep the backups offline



32

White House June 2, 2021 Ransomware Memo to Private Sector (con'd)

- Update and patch systems promptly
- Test your incident response plan
- Check your security team's work; use a third party pen tester to test the security of your systems and your ability to defend against a sophisticated attack
- Segment your networks

Source: https://assets.documentcloud.org/documents/20796933/memo-what-we-urge-you-to-do-to-protect-against-the-threat-of-ransomware17.pdf

See also: https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/

See also: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

33

Ransomware Risk Mitigation

34

General Concerns/Considerations

- Explosion of Attacks
- Hackers Getting Bolder
  - Targets More Critical
  - Effects More Far-Ranging
- Foreign Attacks
- Attacks More Sophisticated
- Prevention v. Response
- Risk Mitigation
- Federal Recommendations – Risk Mitigation Considerations
  - White House Memorandum – June 2, 2021
  - Executive Order – May 12, 2021

35

Risk Assessments/Vulnerability Evaluations

- Prevention/Risk Mitigation
  - Minimize Exposure Via Periodic System Reviews
  - Data Mapping
  - Threat Evaluations
  - Vulnerability Identification
- Goal – To Identify Critical Weaknesses
  - Allocate Limited Resources
  - Minimize Threat Profile
  - Create Response Plans (and Practice Them)
- Payment Considerations – Yes or No??
- Conduct Regular Status Meetings – Key Players
- Cyber Insurance

36

Cyber Controls/Data Security Safeguards

- Data Mapping
  - What Data is Collected/Stored?
  - How Sensitive/Critical Is the Data?
  - Safeguards Should Mirror Sensitivity of the Data
- Types of Safeguards
  - Technical/Administrative/Physical
  - Appropriate to the Nature of the Data (Sensitivity/Value)
  - Modify Per The Deltas Shown in the Assessments
  - Encryption of Data – A Definite Must
- Study Recent Incidents
  - What Weaknesses Exploited There?
  - What Similarities With Your Systems?
- Types of Approaches
  - CIS
  - NIST
  - ISO

37

System/Patch Upgrades and Implementations

- Attacks Over Recent Years
  - Significant Number Failed to Implement Current Upgrades or Patches
  - Timely Upgrades Are Critical To Minimize Ransomware Risks
- Internal Systems Should Be Set Up Accordingly
  - Consider Implementation Testing
  - Timing is Critical
  - Implementation Delays Create Windows For Hackers
- Be Sure to Have Acquisition Protocols In Place
  - Assures Timely Receipt of Patch/Upgrades
  - Monitor Relevant Boards As To Your Systems

38

Vendor/Third-Party Access

- Vendor Access Vulnerabilities
  - Third-Parties That Have Access to Your System
- Impose Your System Security Protocols
  - On All Parties With System Access
  - Verify Compliance on a Regular Basis
- Key Is To Close/Reduce All Windows Into Your System
- Carefully Track All Risk Assessments
  - Audit Third Parties Strategically
  - Minimize Third Party Access

39

Employee Training

- One Component of Security Triad
  - Administrative Protocols
  - Technical Protocols
  - Physical Protocols
- Significant Weakness
  - Target of Phishing Efforts
  - Access For Malware/Ransomware
- Scope of Coverage
  - Importance of Data Security in General
  - Importance to Employer
  - Focus on the Data that Employees Will Encounter
  - Describe Data Incidents/How Employees Would Encounter
  - Review Incident Response Actions
- Sensitize The Employees To Data Issues/Importance

40

System Back-up Practices

- Maintain System Back-ups
  - Store Separate From the Main Systems
  - Maintain Isolated Copies For Several Months
- Key Is To Have Clean Back-ups From Which To Restore Systems
  - Short Cycles Will Increase Risk of Contaminated Back-up Data
  - Lack of Clean Data Forces Consideration of Payment
  - Lack of Clean Data Increases Risk of Business Shutdowns

41

Summary – Best Practices

- Prevention is Key
- Be Proactive
- Keep Cyber Controls/Protocols Current
- Keep Ahead of Your Vulnerability Profiles
- Monitor Trends/Developments
- Implement Your Security Strategies For The Right Reasons
- Be Timely and Aggressive
- Segregate Back-up Data Copies From Main Systems
- Train Your Operational Employees Thoroughly
- Oversee Third-Party Access Windows/Actors Agressively
- Do Not Be Reactive!!!

42

Legal Obligations

43

Legal Requirements -- Federal

- FTC Act
  - General Businesses
  - Deceptive/Unfair Practices
- HIPAA/HITECH – Healthcare Providers/Business Associates
  - Security/Privacy Rules
- SEC – Regulation S-P (“Safeguards Rule”)
- Family Educational Rights and Privacy Act (“FERPA”)
- Fair Credit Reporting Act (“FCRA”)

44

Legal Requirements -- State

- Breach Notification/Security Systems
  - General/Proactive
- State Unfair/Deceptive Trade Laws
  - General/Reactive

- NYDFS Cybersecurity Regulations (effective 3/1/2017)
- Massachusetts Data Regulations

45

State Breach Notification Statutes

- All 50 States Now Have Breach Notification Statutes
- Most Also Have Data Security Requirements
  - Relate to Handling of "PII"
  - Typically Require "Reasonable Security Procedures" That Are "Appropriate To The Nature of the Information"
  - Standard Provides Flexibility Relative to Sensitivity of the Data and Threat Profile of Data Collector
  - "Develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards…"
- *See* Cal. Civ. Code §1798.81.5(b)
- *See* Mass. Reg. 201 CMR 17.03, 17.04

46

General Cyber Preventative Measures

47

Preventive Measures I

- Conduct Detailed Data Audit
  - Identify Your Data – Types/Sources
  - Map Where The Data Is Stored
  - Map The Data Flows
- Identify Your Data Requirements? – How Long Do You Need It?
- Destroy Data When No Longer Needed
  - Business Needs
  - Legal Retention Requirements
- Potential Alternative – Data Anonymization

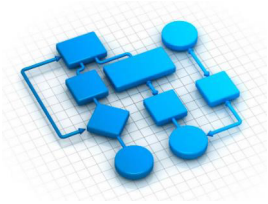
48

Preventive Measures II

- Conduct Detailed Risk Assessment
  - Built on Data Audit
  - Identifies Potential Threats
- Will Give You Solid Profile of Your Activities and Your Vulnerabilities
- This Exercise Is Common Across Sectors
- This Assessment Is the Foundation On Which Cyber Protections Must Be Based

Preventive Measures III

- Implement The “Cyber Triad”
  - Administrative Protocols
  - Technical Protocols
  - Facility Protocols
- Admin – Access Restrictions, Passwords, Incident Response Plans, Business Continuity Plans
- Tech – System Logs, Firewalls, Encryption
- Facility – Security Cards, Temperature/Humidity, Power



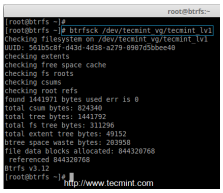
Preventive Measures IV

- Employee Awareness/Training Programs
  - Make Them Aware of the Threat
  - Instruct as to Handling of Email and Attachments
  - Provide Clear Contact Information For Handling
- Robust Email Scanning/Strong Spam Filters
- Segregate Network Components/Locations
  - By Function, Need or Location
  - Keeps Access Limited In Case of Penetration
  - Minimizes Harm From Breach

51

Preventive Measures V

- Keep Firewalls/Other Defenses Current
  - Implement Updates Immediately
  - Review and Implement Software Patches When Issued
- Conduct Regular/Frequent System Scans
  - Make a Regular Event
  - Retain Records of Each Scan
  - Regularly Review System Logs/System Activity Records
- Robust Use of “Least Privilege Principle”
  - No One Receives Complete Access
  - Each Person Receive Access For Their Role Only



52

Preventive Measures VI

- Frequent System Backups (and Secure Them)
  - Segregate From the Network
  - If They Are Hit, …..
- Annual Penetration Tests/Vulnerability Assessments
  - Expose Weak Spots/Gaps in Perimeter
  - Address Vulnerabilities ASAP
- NOTE – Pen Tests Must Be Used In Conjunction With Architecture Assessment (Not A Substitute)
  - To Minimize Problems Assuming a Penetration Occurs
  - Architecture Assumes That A Penetration Has Occurred

53

Preventive Measures VII

- Implement Detailed Incident Response Plans and Business Continuity Plans
  - Base On Potential Contingencies Depending on Types of Data
  - Identify Team Members and Roles (Will Vary Depending on Type of Event/Breach)
  - Include Ransomware
  - Time is of Essence – Practice is Essential (Table Tops)
  - Have Emergency Contacts Identified NOW!!
- Business Continuity Plans
  - Use of Co-Location Facilities
  - Anticipate Possible Events – Weather, Criminal, Technical

54

Preventive Measures VIII

- Conduct Tabletop Exercises
  - Should Parallel Breach Response Efforts
  - Contemplate Various Permutations of Attack
  - Minimum Every 6-12 Months
  - Must Include Each Team Member
- Third-Party Contacts
  - FBI
  - US Attorney
  - Forensics Investigators
  - Legal Counsel
- Bitcoin/Digital Resources??

55

Preventive Measures IX

- Third Party Vendor Management
  - Should Mirror/Parallel Your Own Security Protocols
  - Should Also Mirror/Parallel Your Customer Protocols As Needed
  - Obtain All Evidence of TPV Certifications
  - TPV Reps/Warranties Not Enough
- Be Sure To Obtain Customer Requirements In Writing To Correctly Impose On Vendors

56

Preventive Measures X

- Consider Cyber Security Insurance
- Review Proposed Terms Carefully
  - May Not Cover Ransomware/Cyber Extortion
  - If There is Coverage, Scan The Conditions Carefully
- Notice May Be Mandatory Before Payments Made
- Note That Retentions Often Exceed The Ransom
- Detailed Due Diligence May Be Necessary Before Payment
  - Confirm The Validity of the Threat
  - Confirm The Scope and Lack of ANY Alternative Resolution
  - Mandatory C-Suite Approval of Ransom Payment

Law Enforcement Resources

- FBI
- US Attorney
- US Secret Service
- Local Police
- Will Likely Have To Work With IT/Forensics Teams

What is “Reasonable”?

Federal/International Levels

- Graham Leach Bliley
  - Financial
- HIPAA
  - Healthcare
- FTC
  - General Business
- GDPR
  - EU Data

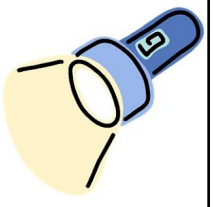
Legal Requirements -- State

- Breach Notification/Security Systems
  - General/Proactive
- State Unfair/Deceptive Trade Laws
  - General/Reactive
- NYDFS Cybersecurity Regulations (effective 3/1/2017)
- Massachusetts Data Regulations
- Proposed Insurance Statutes – Uniform Cyber Requirements
  - Data Security
  - Breach Notification

61

State Breach Notification Statutes

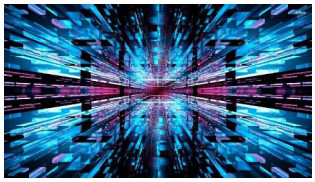
- 50 States Have Breach Notification Statutes
- Most Also Have Data Security Requirements
  - Relate to Handling of "PII"
  - Typically Require "Reasonable Security Procedures" That Are "Appropriate To The Nature of the Information"
  - Standard Provides Flexibility Relative to Sensitivity of the Data and Threat Profile of Data Collector
  - "Develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards…"
- *See* Cal. Civ. Code §1798.81.5(b)
- *See* Mass. Reg. 201 CMR 17.03, 17.04



62

Reasonable Security Standards -- CA

- CA AG – February 2016
- Failing to Implement the CIS Critical Security Controls "Constitutes a Lack of Reasonable Security"
- Other Endorsements:
  - NIST Cybersecurity Framework
  - National Governors Association
  - European Telecommunications Standards Institute
  - UK Centre for the Protection of National Infrastructure
  - National Highway Traffic Safety Administration
- *See* https://www.cisecurity.org/controls/



63

New York Dept. Financial Services Regulations

- Effective on March 1, 2017 – 23 NYCRR 500
- Applicable to Institutions Licensed Under NY:
  - Banking Law
  - Insurance Law
  - Financial Services Law
- Each *Covered Entity* shall maintain a *cybersecurity program* designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems.
- The *cybersecurity program* shall be based on the Covered Entity's *Risk Assessment.*

64

NYDFS – Part II

- Identify Internal and External Risks
- Implementation of Cyber Defenses
- Implementation of Cyber Policies
- Cyber Triad
  - Administrative
  - Technical
  - Physical
- Appointment of CISOs
- Regular Testing and Assessment of Program
- Audit Trails
- Implementation Flexibility

65

Federal Trade Commission

- More Aggressive Enforcement
  - Uber, Vizio, LabMD, Privacy Shield certification
- Implementation of Cyber Defenses/Programs
- Major Fronts
  - Use of Encryption
  - Autonomous Cars (Note CA Regulations)
  - Internet of Things
  - Privacy by Design
  - Credit Reporting Agencies

66

Securities and Exchange Commission

- Regulation S-P
- New Cyber Specialty Unit
  - Market manipulation involving false information spread through electronic and social media
  - Hacking to obtain material nonpublic information
  - Misuse of distributed ledger technology
  - Misconduct perpetrated via the dark web
  - Intrusions into retail brokerage accounts
  - Cyber-related threats to trading platforms and other critical market infrastructure

67

Recent SEC Cyber Initiatives

- The SEC's examination program has issued 3 risk alerts related to cybersecurity.
- On Aug. 7, 2017 the SEC issued its most recent discussing: governance and risk assessment; access rights and controls; data loss prevention; vendor management; training; and incident response.
- Notably, the SEC also included a section on the "Elements of Robust [Cyber] Policies and Procedures" to provide guidance on best practices.
- FINRA's Feb. 2015 "Report on Cybersecurity Practices" also provides broker-dealers with a strong resource.
- SEC Enforcement will be increasing its focus. On Sept. 25, 2017, the SEC announced the creation of a "Cyber Unit" to focus on targeting cyber-related securities law violations.
- The SEC Enforcement Director recently stated that "[t]he greatest threat to our markets right now is the cyber threat."

68

HHS/OIG

- More Aggressive Enforcement
- Increased Fines/Penalties
- Emphasis on Encryption
  - Decisions Not Sympathetic to Lack of Encryption
  - Encryption Now Cheaper and Devices More Powerful
  - Less Rationale For Decisions to Avoid Encryption
- Still Technically a “Safe Harbor”

69

Business Self-Regulation – PCI DSS

- PCI-DSS (Version 3.2.1)
  - Announced in May 2018
  - Version 3.2 Expired in December 2018
- Scope – Credit Card Data Security
  - Requirements -- 12
  - Each Requirement Broken Down Into Multiple Sub-Parts
  - Each Requirement Has Testing and Guidance Parameters
- Compliance
  - Required By All Merchants Regardless of Size
  - Scrutiny Level Rises As Transaction Quantities Increase

70

Business Self-Regulation – PCI DSS

- Requirement 1
  - Install and Maintain Firewall Configuration to Protect Cardholder Data
- Requirement 2
  - Do Not Use Vendor-Supplied Defaults For System Passwords/Other Security Parameters
- Requirement 3
  - Protect Stored Cardholder Data
- Requirement 4
  - Encrypt Transmission of Cardholder Data Across Open/Public Networks

71

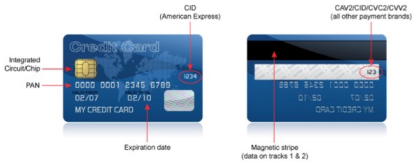
Business Self-Regulation – PCI DSS

- Requirement 5
  - Protect All Systems Against Malware and Regularly Update Anti-Virus Software or Programs
- Requirement 6
  - Develop and Maintain Secure Systems and Applications
- Requirement 7
  - Restrict Access To Cardholder Data By Business Need to Know
- Requirement 8
  - Identify and Authenticate Access to System Components

72

Business Self-Regulation – PCI DSS

- Requirement 9
  - Restrict Physical Access to Cardholder Data
- Requirement 10
  - Track and Monitor All Access to Network Resources and Cardholder Data
- Requirement 11
  - Regularly Test Security Systems and Processes
- Requirement 12
  - Maintain a Policy That Addresses Information Security For All Personnel



73

CIS Controls

74

CIS Controls v7.1

- CA AG – February 2016
- Failing to Implement the CIS Critical Security Controls "Constitutes a Lack of Reasonable Security"
- CIS Controls v7.1 – 4/1/2019
  - Implementation Groups – IG1, IG2 and IG3
  - Sub-Controls per IG's
  - Provides general goals subject to specific risk assessments
- *See* https://www.cisecurity.org/controls/

75

CIS Controls v7.1

- IG1
  - Small-to-Medium Size
  - Limited IT/Cyber Expertise
  - Limited Tolerance for Downtime
  - Data Sensitivity – Low (Employee/Financial)
- IG2
  - Specific Employees For IT Management/Protection
  - Segments with Differing Risk Profiles – Some May Have Regulatory Demands
  - Data Sensitivity – Medium (Sensitive Client and/or Company Data)
  - Short Service Interruptions Possible
  - Major Concern -- Loss of Public Confidence

76

CIS Controls v7.1

- IG3
  - Specific Employee Experts For Differing Cyber Facets
    - Risk Management
    - Pen Testing
    - App Security
  - Data Sensitivity – High (Subject to Regulatory Oversight)
  - Service Interruptions Not Possible
  - Successful Attacks Can Affect Public Welfare
  - Sophisticated Attacks Very Possible

77

CIS Controls v7.1

- Control Levels
  - Basic
    - CIS Controls 1 - 6
  - Foundational
    - CIS Controls 7 - 16
  - Organizational
    - CIS Controls 17 - 20

Basic

78

CIS Controls -- Basic

- Control 1 (8 sub-controls)
  - Inventory and Control of Hardware Assets
- Control 2 (10 sub-controls)
  - Inventory and Control of Software Assets
- Control 3 (7 sub-controls)
  - Continuous Vulnerability Management
- Control 4 (9 sub-controls)
  - Controlled Use of Administrative Privileges
- Control 5 (5 sub-controls)
  - Secure Configuration for Hardware and Software on Mobile Devices
- Control 6 (8 sub-controls)
  - Maintenance, Monitoring and Analysis of Audit Logs

CIS Controls -- Foundational

- Control 7 (10 sub-controls)
  - Email and Web Browser Protections
- Control 8 (8 sub-controls)
  - Malware Defenses
- Control 9 (5 sub-controls)
  - Limitation and Control of Network Ports, Protocols and Services
- Control 10 (5 sub-controls)
  - Data Recovery Capabilities
- Control 11 (7 sub-controls)
  - Secure Configuration for Network Devices (Firewalls, Routers and Switches)
- Control 12 (12 sub-controls)
  - Boundary Defense

CIS Controls – Foundational (cont'd)

- Control 13 (9 sub-controls)
  - Data Protection
- Control 14 (9 sub-controls)
  - Controlled Access Based on the Need to Know
- Control 15 (10 sub-controls)
  - Wireless Access Control
- Control 16 (13 sub-controls)
  - Account Monitoring and Control

81

CIS Controls -- Organizational

- Control 17 (9 sub-controls)
  - Implement a Security Awareness and Training Program
- Control 18 (11 sub-controls)
  - Application Software Security
- Control 19 (8 sub-controls)
  - Incident Response and Management
- Control 20 (8 sub-controls)
  - Penetration Tests and Red Team Exercises

82

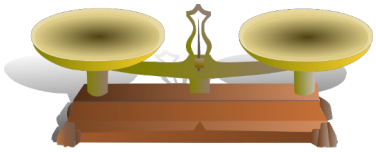
CIS Controls – Spread Across Groups

- Basic Sub-Controls – 47
  - IG1 – 11 (23.4%)
  - IG2 – 38 (80.8%)
  - IG3 – 47 (100%)
- Foundational Sub-Controls – 88
  - IG1 – 22 (25.0%)
  - IG2 – 70 (79.5%)
  - IG3 – 88 (100%)
- Organizational Sub-Controls – 36
  - IG1 – 10 (27.7%)
  - IG2 – 32 (79.5%)
  - IG3 – 36 (88.8%)

83

Ultimate Goal – Balancing Test

- Resources Are Not Unlimited
- Goal/Target
  - Risk Minimization
  - Not Risk Elimination
- How To Utilize Assets Wisely
- Considerations
  - Size of Enterprise
  - Type of Data – Sensitivity/Scope/Flow
  - Threats – Resources/Capabilities
  - Risk Vulnerabilities



84

In Conclusion – One Word

ENCRYPT

85

QUESTIONS??

86

Kenneth K. Dort

Partner
Intellectual Property/Information Technology/Data Governance
Chicago
+1 312 569 1458
kenneth.dort@faegredrinker.com

Ken Dort is a preeminent resource on mission-critical data security issues and is consulted often for immediate counsel on high-stakes data breaches, as well as for guidance and strategy on the privacy and other legal implications of new technologies. Ken is a recognized adviser to clients around the world on data security and privacy practices and compliance needs arising under federal, state, provincial and international laws and industry standards. He also is a powerful litigator in the courtroom, a deft negotiator with regulators and a valued counselor on software development and integration.

Over his 30-year career, Ken has focused on the ways that law and regulation frame the development of new technology. He is engaged by some of the world's largest companies to stem and mitigate major data breaches and ransomware attacks, including those involving credit card information and employee, customer and patient data. He is called on frequently to create or improve data security and privacy protocols for highly sensitive information, devices and mobile applications.

Ken also works with leading forensic investigators to assess client information systems and security protocols and addresses issues and compliance needs that arise under cyber security laws and standards in the US, EU, Canada, Japan, Australia, Brazil and the Middle East.

Ken is certified (CIPP/US, CIPP/EU and CIPP/C) by the International Association of Privacy Professionals.