

SENG 460 / ECE 574

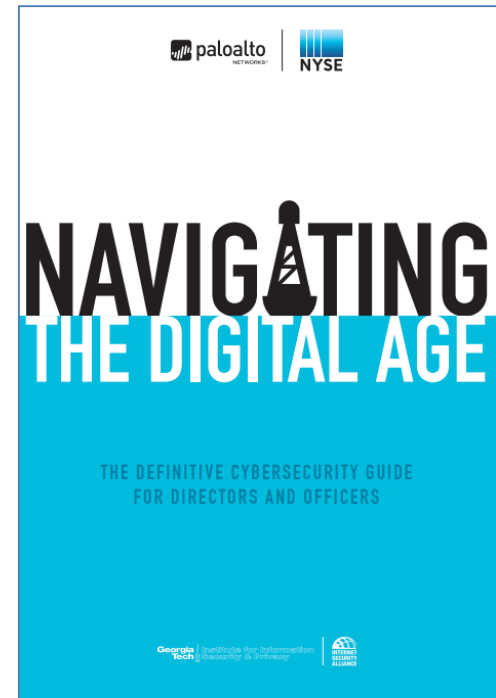
Practice of Information Security and Privacy

Navigating the Digital Age

Reading Review

Gary Perkins, MBA, CISSP

garyperkins@uvic.ca



Foreword

- cybersecurity has never been as imperative
- issue can't be taken for granted
 - 1) technology platforms are bigger targets
 - 2) amount/value of data grown exponentially
 - 3) interconnectedness of the world makes it easier for people to steal or disrupt
 - 4) perpetrators more sophisticated/organized/
funded/elusive
- “the data is a gold mine for criminals”
- data is the new oil



Foreword

- protecting data and systems is core to business
- ensuring an effective security program
 - be open and honest about effectiveness of security program with the board
 - cybersecurity begins at the top, executives must be aware of risk
 - security should be built in from the ground up
 - security is not a destination but a journey; **assume compromise**
 - can't be fixed by one organization, need all together (hyperconnectedness)
 - collaborate and share information (strength in numbers)
 - “cybersecurity needs to be part of the fabric of every company and every industry, integrated into every business process and every employee action”
 - references to attack surface, battle for talent, stateful inspection,

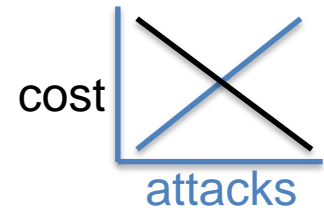
no organization is immune



University
of Victoria

Chapter 1

- breaches are putting our digital lifestyle at risk
 - increasing reliance on systems
 - increase in cyberattacks
- decreasing cost of computer power means easier to launch frequent/sophisticated attacks
- don't need to have the skills
 - can use someone else's work or hire someone else
- defenders are relying on old technology



Chapter 1

- attack surface increasing
- strategy must be to decrease likelihood required for attacker to perform a successful attack (how?)
- total prevention is not possible
 - no organization globally is immune to attack
- wise organizations assume breach
 - even if hasn't happened it is a helpful mindset
- goal is to reduce risk to an acceptable level

Chapter 1

- concept of networks has changed (cloud, IoT)
- security architecture of the future
 - advanced security systems designed on knowledge of what/who is using the network
 - capabilities natively integrated into platform
 - platform part of larger global ecosystem
 - security posture consistent regardless where data resides
- successful leaders must understand need to assess risk and allocate resources and effort
- require continuous improvement to combat the threat

Chapter 1

- many attacks start with poor processes/human error
- phishing example
 - who would fall for it? whose fault is it? should we blame the victims?
 - spearphishing, whaling, smishing, vishing; targeting wire-transfers – EFT – example
- companies need to collaborate and force attackers to come up with new attacks each time
 - next generation technology, improvements in processes and training, real-time sharing of threat information
 - reduce # of successful attacks & restore digital trust

Chapter 2

- what are the three T's? technology, threat, trust
- references to hackers, phishing, identity theft
- references to Sony, Target, Anthem, US OPM, Uber
- forces changing the risk profile
 - cloud computing, mobility, big data, social media, virtualization, IoT
- individuals, hacktivists, org crime, nation-states
- reference HBGary, Target, JPMorgan Chase, Sony
- motives: embarrass, steal info, disrupt ops, destroy

Chapter 2

- questions to start asking for breaches
 - is the company still around?
 - long lasting impact to reputation?
 - who was responsible? (eg. Equifax)
- reference to cyber insurance
 - discuss
- ability for successful attack to undermine trust
- what does an organization have to lose?
 - intellectual property? customers? share price? trust?

Chapter 2

- treat cyber risk as an enterprise risk
- understand legal implications
- discuss cyber at board meetings
- measurable cybersecurity plan
- plan to address cyber risks
 - avoid, accept, mitigate, transfer (via insurance)
 - can you really transfer the risk?
- cyber insurance – quotes, payout, examples

Chapter 3

- cyber governance best practices
- IT governance the responsibility of BoD and exec
- security controls, risk mgmt, protect PII in cloud
- ISACA, ITIL
- COBIT, NIST, NERC, HIPAA
- BS 7799 – ISO 17799 – ISO 27001, ISO 27002
- SOX, SAS70/SSAE16, PCI

Certification/Accreditation

- **certification**

- evaluation of security components and compliance for the purpose of accreditation
- process may use safeguard evaluation, risk analysis, verification, testing, and auditing techniques to assess the appropriateness of a specific system
- corresponding documentation will indicate the good, the bad, and the ugly about the product and how it works within the given environment

- **accreditation**

- formal acceptance of adequacy of system's overall security & functionality by mgmt
- confirms management understands level of protection system will provide
- understands the security risks associated

- **systems continually change and evolve so certification and accreditation should also**

- new systems and material changes to existing ones

Chapter 3

- enable executive to understand maturity of cybersecurity program
- adopt a risk-based approach
 - set direction of investment decisions
 - ensure conformance with internal and external requirements
 - foster a security-positive environment

Chapter 3

- review performance in relation to business outcomes
- inform the board of security issues
- reference to Target, lawsuits, Wyndham
 - exec and BoD failed to protect company's data and ensure robust IR plan
- risk of headlines
- reference to CISO reporting to the CIO
 - is this a conflict of interest?
- CIOs and CISOs need better exec and BoD skills

Chapter 3

- 12 practices for cyber governance:
 - governance structure, vulnerabilities, security program, legal/financial exposures, tone from top, roles/responsibilities, shared responsibilities, review/approve budgets, trusted advisor, cyber insurance
- 12 practices for integrating cyber security
 - business strategies/objectives/needs, asset inventory/classification/risk, legal requirements, vendors, best practices, metrics, risk assessment, cyber risk, system architecture, technical tools – integrated data, annual training, aware of changes

Chapter 4

- investor's perspectives on cyber risks
- reference to Target, shareholders, BoD, C-level
 - “failed to provide sufficient oversight of the risks facing the company that potentially led to the data breach”.... BoD voted out
- $< \frac{1}{2}$ of boards have skills to manage cyberthreats
- 43% have unacceptable skills and knowledge to manage innovation and risk in the digital world

Chapter 4

- reference to Home Depot
 - company expanded the incident response team
 - Jan 2014 accelerated payment security project
 - takes raw payment card info and scrambles to make unreadable
 - ways to protect data:
 - encryption
 - tokenization
 - obfuscation
 - new chip and pin tech
 - executive committee, adding CISO, enhanced training
- loss of investor confidence

Chapter 5

- cyber risk measurement – cyber risks are imminent cost of doing business
- cybersecurity is already part of BoD agenda
- cloud-based solutions – more secure? less secure?
- 50% of customers switch brands if compromise
- \$445 billion – annual cost of economic espionage
- \$140 million – costs of Target breach

Chapter 5

- how much should you spend on cybersecurity?
 - should not spend \$10 million securing something unless you can show, for example, that breach costs you \$1 million and will happen 10 or more times
- probability model, hacker model, attack model, asset and loss model, security model, company model
- raise awareness of cyber risks
- no silver bullet – assess assets, existing controls, vulnerabilities, know attackers and threats

Chapter 6

- no organization is immune to attack
 - military does not have enough security to repel
- attackers are not focused only on zero-day attacks
 - they are counting on organizations being too distracted to patch
 - reusing old code – virtually no-one writes or develops from scratch
- attacks are not just on laptop and desktop computers
 - attacks are on mobile phones, IoT, cars
- attacks are more targeted than ever
 - APT is Advanced Persistent Threat
 - author calls it Average Persistent Threat

Chapter 6

- vulnerability exists
- vulnerability is discovered
- vulnerability is reported
- vulnerability is communicated
- vulnerability is theoretical or exploit exists
- see exploit attempted “in the wild”
- vulnerability successfully exploited


Chapter 6


- cyberattacks are relatively cheap and easy to access
 - can hire attackers (see next 3 slides)
- we successfully prosecute less than 2% of cyber criminals
- concept of shrinkage with retail organizations
 - cost of doing business – 5% of inventory walking out the back door
 - if it costs 6% to mitigate then not worth it
- important for organizations to know their “crown jewels”
 - what are the critical systems and data


Reliable and Trusted server & network testing!
Best Stress testing since 2010!

[SEE ALL PLANS & PRICES](#)


FEATURES


 Unlimited Testing

 Great User Experience

 24/7 Live Support

 Easy Customizable

 Flexible Pricing

 VIP Support

 Affordable Plans

Excellent Stress Testing Services!

With Rage Booter, you never have to worry about power! We monitor our servers 24/7 to provide you a pure and strong attack to any target.

- ✓ Fast and Secure Stress Testing!
- ✓ Ticket & Live Support!
- ✓ A Variety of revolvers from Cloudflare to Skype, we have it all!
- ✓ We have been open since 2010 so you can feel peace at mind that we are not going anywhere!

Instant Attacks!

Unlike other stressers who use SSH2, We utilize IRC (Internet Relay chat) to send all attacks. Attacks are instant and sent fast using this.

Membership Plans

1 Day Trial Price: \$1 Max Boot Time: 120 Seconds Text Bomber: 60 Texts Concurrents Attacks: 1 SIGN UP	Bronze Monthly Price: \$2.5 Max Boot Time: 300 Seconds Text Bomber: 60 Texts Concurrents Attacks: 1 SIGN UP	Silver Monthly Price: \$5 Max Boot Time: 600 Seconds Text Bomber: 120 Texts Concurrents Attacks: 1 SIGN UP	Gold Monthly Price: \$7.5 Max Boot Time: 900 Seconds Text Bomber: 240 Texts Concurrents Attacks: 1 SIGN UP
Bronze Lifetime Price: \$10 Max Boot Time: 300 Seconds Text Bomber: 60 Texts Concurrents Attacks: 1 SIGN UP	Silver Lifetime Price: \$15 Max Boot Time: 600 Seconds Text Bomber: 120 Texts Concurrents Attacks: 1 SIGN UP	Gold Lifetime Price: \$20 Max Boot Time: 900 Seconds Text Bomber: 180 Texts Concurrents Attacks: 1 SIGN UP	Platinum Monthly Price: \$25 Max Boot Time: 3000 Seconds Text Bomber: 240 Texts Concurrents Attacks: 2 SIGN UP
Platinum Lifetime Price: \$50 Max Boot Time: 3000 Seconds Text Bomber: 300 Texts Concurrents Attacks: 2 SIGN UP	Ultimate Monthly Price: \$62.5 Max Boot Time: 5000 Seconds Text Bomber: 300 Texts Concurrents Attacks: 2 SIGN UP	Omega Monthly Price: \$100 Max Boot Time: 9000 Seconds Text Bomber: 300 Texts Concurrents Attacks: 3 SIGN UP	Ultimate Lifetime Price: \$125 Max Boot Time: 5000 Seconds Text Bomber: 300 Texts Concurrents Attacks: 2 SIGN UP
Omega Lifetime Price: \$200 Max Boot Time: 9000 Seconds Text Bomber: 500 Texts Concurrents Attacks: 3 SIGN UP			

THIS WEBSITE HAS BEEN SEIZED

This domain has been seized by the Federal Bureau of Investigation pursuant to a seizure warrant issued by the United States District Court for the Central District of California under the authority of 18 U.S.C. §1030(i)(1)(A) as part of coordinated law enforcement action taken against illegal DDoS-for-hire services.

This action has been taken in coordination with the United States Attorney's Office of the District of Alaska, the Department of Justice Computer Crime and Intellectual Property Section, and



For additional information, see the FBI Public Service Announcement I-101717b-PSA,
<https://www.ic3.gov/media/2017/171017-2.aspx>

Chapter 6

- costs of a data breach, switching costs
 - 2014: 3.5M, \$145
 - 2015: 3.79M, \$154
 - 2016: 4.00M, \$158
 - 2017: 3.62M, \$141
 - 2018: 3.86M, \$148
- average size of data breaches increased
- 6-12 months after Target & Sony breaches the stock prices were up 22 and 26%

Chapter 6

- Obama desire for minimum standards for cybersecurity
 - did not pass
 - 2013 Executive Order for public-private partnership
- Cybersecurity becoming even more serious
 - insecure system becoming weaker
 - attack community more sophisticated
 - massive economic incentives over defenders
 - government methods to fight cyber crime have not matured to address the dynamic nature of this threat
- road to creating sustainably secure cyber

Chapter 7

- breach statistics
 - 60% of 80k security incidents attackers were able to compromise an organization in minutes
 - *author suggests 1/3 were discovered within days*
 - research suggests 196-206 days for companies to detect a breach
- cybersecurity risk can be effectively managed with integrated approach to risk management
- security is not just the role of the CIO and CISO
 - example: Target reference and Board of Directors
 - it is the responsibility of corporate officers and the board

Chapter 7

- managing cybersecurity must be ongoing and iterative – not one-time/infrequent or check-the-box
- no such thing as perfect security
- don't want to constrict ability of business to operate
- although security seems more technical the outcome is still the same – eliminate, mitigate, transfer, or accept risk affecting the company's future
- not all risk can be eliminated

Risk Register

Risk	Definition	Inherent risk	Risk trend	Key risk mitigation strategies	Residual risk	Owner
Network Security	Insufficiently proactive approach on identification of threats and vulnerabilities in network infrastructure and timely mitigation may result in network outages and exposure					
Data Security	Insufficient application of adequate security controls, heightened by increased risks from ransomware and profit-driven cyber criminals results in an inability to identify and mitigate unauthorized access, disclosure, modification, deletion of sensitive data					

Chapter 7

- risk framing and assessment, controls assessment, risk decision making, residual risk sign-off, risk monitoring
- risk appetite, risk register, regular review, conscious acceptance of risk
- accountability not about who to blame when something goes wrong
- ensures formal risk management process is followed
- need a clear understanding of corporate risk tolerance

Questions the CEO/Board are asking security teams:

1. do you know what our critical systems and data are?
2. what are the security controls in place?
3. are the controls sufficient to mitigate risk to an acceptable level?

Questions the CEO/Board should be able to answer:

1. what are the key cybersecurity risks affecting your industry/organization?
2. is your organization aligned with an existing industry security standard (ie. ISO or NIST)
3. what is your current capability/maturity rating?
(0 – Not Implemented, 1 – Initial, 2 – Repeatable, 3 – Defined, 4 – Managed, 5 – Optimized)
4. what is your desired capability/maturity rating?
5. do you have a plan to reach the desired level?
6. how frequently do you receive plan updates?
7. is security a recurring item on the board agenda?

Chapter 7

- what is secure enough?
 - cybersecurity programs must continually mature
 - is there a consistent understanding of company's tolerance for cybersecurity risk?
- risk register reviewed? monitored? when threats, vulnerabilities, or conditions change?
 - new risk treatment plan?
- effective cyber incident response plan? exercised?
lessons learned?

Chapter 7

- effective communication is important
 - create a company culture of cybersecurity risk is critical
 - employees must understand the basics
 - employees must be empowered and rewarded for identifying cybersecurity issues
- when cyberthreats and vulnerabilities are regularly evaluated, employees are empowered to report issues and business is aware of the impacts
- continuous evaluation of the risk management process

Chapter 8

- cyber attacks and data breaches accelerating in number and frequency
- boards that choose to ignore or minimize the importance of cybersecurity do so at their own peril
 - cybersecurity discussed at 80% of all board meetings
 - 34% are confident about their companies' ability to defend
- protecting the corporation's crown jewels is essential
- references to Target, Wyndham, TJX Companies, Heartland and 110, 130, 45 million credit cards

Chapter 8

- cybersecurity disclosures
 - disclose or not? vs mandatory breach notification
 - when to disclose? consider Equifax example
- importance of awareness and appointing a CISO
 - those that do have less incidents and less loss per incident
- have a committee
 - cybersecurity presentations should not be overly technical
- plan implementation and enforcement, tabletop exercises, required training, monitor compliance, regular patching

Chapter 9

- risks associated with cyber attacks are a large and growing concern
 - SEC will use authorities already on the books to promote cybersecurity in public companies
 - SEC will use every tool it has to combat cyber risks
- cyber disclosures have an effect on corporate reputations and stock price, would-be attackers info about vulnerabilities and trigger shareholder and other litigation

Chapter 9

- trends
 - all cyber incidents to be disclosed
 - staff will research cyber incidents and ask about them
 - no currently existing securities law or rule expressly requires cyberattacks to be reported on (voluntary)
- consider – you are at an organization and have a breach – how conflicted are you whether to report?
 - why disclose if you don't have to?
 - are you going to disclose anyway?
 - is the incident likely to become widely known?

no organization is immune

be prepared for when it happens

Chapter 10

- cyber derived from Greek word kybernan from which the word govern also derives
- corporate assets have changed significantly – 80% of Fortune 500 is IP - digitization of assets
- in cyber world legal superstructure is dramatically underdeveloped
- cyber risk must be considered central feature to business process

Chapter 10

- corporate spending has doubled and more than \$100 billion a year
 - DHS has “only” \$1 billion for cybersecurity
 - total US government is \$16 billion
- principles:
 - understand cybersecurity is an enterprise risk management issue
 - directors must understand the legal implications of cyber risk
 - board members need access to cybersecurity expertise
 - expectation of enterprise wide cyber risk management framework
 - method to assess damage of cyber event

Chapter 10

- cybersecurity is the top issue boards face
- cybersecurity as IT is flawed
 - single biggest vulnerability is people (single biggest asset too?)
 - employees often poorly trained, distracted, angry, or...
 - ongoing cybersecurity training is key

Chapter 11

- cybersecurity leaped to the top of the agenda
 - no-one can prevent all cyber breaches
 - issue is enterprise risk not technical solution
- questions:
 - has organization addressed cyber risk? what steps?
 - have you prioritized? aligned with strategy?
 - actions to mitigate cyber risks? test incident response?
- 6 areas:
 - inclusive board level discussion, proactive cyber risk management, risk-oriented prioritization, investment in human defenses, assessments of third-party relationships, incident response policies and procedures

Chapter 11

- claim: infinite number of cybersecurity measures in which a company can invest
- claim: often most critical assets are obvious
- should we hire “white hat hackers” to test our defenses?
- should we test employees anti-phishing awareness?
- educate employees and engage entire enterprise on incident response
 - delayed bumbling response to a security breach is what leads to increased data loss, exposure to regulatory action, and reputational damage

Chapter 11

- board level questions:
 - What are organizations' policies/procedures to rapidly identify breaches
 - How are all employees empowered to monitor and report/respond?
 - How are we triaging/escalating once an incident is detected
 - How is incident response integrated into IT operations
 - What are we doing to align our cyber responses to business requirements and ensure all parts of business understand their roles
 - How does our response plan match up with our threat intelligence?
- Are we characterizing our risk in a way that is consistent with most



Chapter 11

- no-one likes surprises – especially not boards
 - organizations should be prepared in advance for incidents
 - “experience so far suggests that the only companies with truly top-grade, board-level cybersecurity plans are those that have experienced an unpleasant surprise in the form of a bad breach”

Chapter 12

- “it’s what you don’t know that can hurt you”
 - accept that breaches will happen
 - board’s job is to provide reasonable oversight of risk not to manage it
 - strong market where hackers sell data to others
 - this is big business, there is money to be made
 - sellers offering money back guarantees
- threat actors have different motivations, access to resources, level of sophistication

Chapter 12

- mature security strategy
 - determine what needs protecting and who holds the keys
 - identify and protect the assets they must protect
 - where are the assets located
 - “administrator passwords are gold to cybercriminals”
 - prevention is not an endgame
 - no one piece of technology can provide a complete defense
 - good security program assumes that at some point prevention will fail
 - detection is important
 - are we compromised? would we know? how?
 - you can't defend with your eyes closed
 - visibility is key

Chapter 12

- mature security strategy (continued)
 - stay a step ahead: the future won't look like the past
 - apply threat intelligence – tells them intents and capabilities of attackers
 - educate and train vigilant employees
 - employee awareness and training programs
 - organize information security teams for success
 - teams need to have many different skillsets
 - measure effectiveness not compliance
 - security testing
 - compliance should be a by-product of an effective security program
 - emphasize process as much as technology

Chapter 12

- companies are targeted 24/7 365 days a year
 - cybersecurity risk is an enterprise risk not a function of IT
 - [[are you tired of hearing this yet?]]
 - what is the company protecting? how well are they organized to defend the assets? manpower/capability?
 - author recommends:
 - determine vulnerabilities through testing
 - increase visibility to detect attackers
 - use threat intelligence to predict/mitigate attacks
- ensure to resource activities effectively

Chapter 13

- disaster response
 - shouldn't exchange business cards during an emergency
 - meaning you need to be proactive, make introductions before there is a problem
- severe lack of understanding about real risks behind headlines
- 80% say security is discussed in most or every

Chapter 13

- boards are increasingly looking at the CEO and executive members to step up
- as the CEO your job is to balance risk and reward in your company
- what is the current level of cyber risk? what is our plan to address?
- how is executive informed of cyber risk?
- how do we apply industry standards, best practices?

Chapter 13

- how many/types of cyber incidents do we detect?
what is the threshold for notifying executive?
- how comprehensive is cyber incident response plan?
how often is the plan tested?
- critical for CEOs to lead involvement of cyber risks in risk management
- involve CIO, CSO, CISO in conversation from the beginning

Chapter 13

- make sure cyberthreats not seen as ‘someone else’s problem’
- cyberthreats are very real
- tools are regularly sold on the online black market
- no solution is 100%
- develop an incident response plan and regularly test it
- understand the impacts of cyber incidents
- identify your crown jewels – critical assets and data

Chapter 13

- must balance risks and rewards of your decisions and investments
- cyberthreats seem to be an issue of fear for boardrooms
- need to get to a point where cybersecurity is a normal part of business operational plan

Chapter 14

- cybersecurity programs address risk that includes sophisticated attacks
- boards and C-suites don't have cybersecurity skills
- threat landscape is evolving
- platforms holding sensitive data are changing
- cybersecurity should not consist of an annual review
- primary risk to cyber assets is a cyber attack
- “We must know ourselves and our enemies and select a strategy to positively influence the outcome of the battle. There is no reason to fear the attack but there is reason to be concerned about our readiness to defend ourselves from the attack and respond appropriately.”

Chapter 14

- when will the cybersecurity program be completed?
never
- it is a process and not an endpoint
- it is a journey, not a destination
- 5 step process: plan, protect, detect, respond, adjust
- asset inventory, risk assessment, governance
- are your most important systems and data deployed in
protected zones?

Chapter 14

- what are your top 3 most important business processes?
- what systems support those functions?
- does the way your CIO answers match your understanding of critical systems?
- Tier 1: executive leadership
- Tier 2: business management
- Tier 3: systems management

Chapter 14

- risk management is to drive selection of adequate and rational controls and assign responsibilities to manage them
- comprehensive program addresses administrative, physical, and technical controls
- cyberinsurance is becoming increasingly popular way to transfer risk
- outcome for program is expectation that organization can defend its assets from cyber attack

Chapter 14

- executive roles
- business unit roles
- systems management roles
- cybersecurity programs are often a work in process for several years
- best program is one the staff and partners will execute
- magic is in the ability of organization to manage solutions to mitigate risks

Chapter 14

- maintenance of systems and security controls often go underfunded
- cybersecurity programs moved from static defenses to active defenses
- no program is perfect
- continuous monitoring and reporting are important
- plan, protect, detect, respond, adjust

Chapter 15

- companies increasingly use consumer data to stay competitive
- consumers willingness to share data depends on trust
- **enabler of the data economy is the data itself**
- **“data is the new oil”**
- companies gain consumers’ trust and confidence through transparency about personal information they gather

Chapter 15

- **privacy has different meaning to stakeholders based on context, societal norms, geographical location**
- **no consensus definition of privacy**
- variations of personal information
 - self-reported data
 - digital exhaust
 - profiling data

Every minute

Facebook users share nearly 2.5 million pieces of content.

Twitter users tweet nearly 300,000 times.

YouTube users upload 72 hours of new video content.

Amazon generates over \$80,000 in online sales.

Chapter 15

- **privacy**
 - **appropriate collection, use, and sharing of personal information**
- **security**
 - **protecting such information from loss or unintended or unauthorized access, use, or sharing**
- consumers are more likely to buy from companies they believe protect their privacy

Chapter 15

- companies are advertising the importance of privacy and making it a differentiator
- right to be forgotten
 - precedent for removing information from search results that are no longer relevant or not in public interest
- compliance is costly and complicated
- growing data = growing target for “hackers”

Chapter 15

- build privacy considerations into products and services
- create easy-to-understand consumer-facing policies
 - average is 2400 words and takes 10 mins to read
 - policy should state
 - 1) **personal info you will collect**
 - 2) **why it is collected and how it will be used and shared**
 - 3) **how you will protect the data**
 - 4) **explanation of consumer benefit from collection, use, sharing, and analysis of data**

EXAM!

EXAM!

EXAM!

Chapter 15

- **companies should give clear and easy opt-out at every stage**
- develop clear internal data use and retention guidelines
- limit internal access to databases
- create procedure for cyberattacks
- link it to the consumer privacy policy

Chapter 15

- privacy by design
 - developed by Ontario Privacy Commissioner Ann Cavoukian
- communicate your good (privacy) work
 - all actions to protect consumers' privacy should be communicated
 - **publish data principles that communicate how data is gathered, protected, and shared**

Chapter 16

- cybersecurity has been considered the realm of the IT department for too long; it is not just an IT problem
- **data is a core asset of the business**
- data's value to criminals has the attention of regulators consumed with consumer privacy and safety
- senior management is responsible for determining cyber risks and implementing a compliance program

Chapter 16

- board is responsible for overseeing risk identification process and evaluating whether program is effective
- disconnect between board, C-suite and operations poses a significant challenge
- cybersecurity oversight is risk management oversight
- purpose of risk management is to identify and mitigate risks to an acceptable level
- **risk appetite**

Chapter 16

- data risks
 - risk of financial loss, value loss
 - business/operational disruption, loss of productivity
 - loss or compromise of assets/info, data, intellectual property
 - compliance with legal, regulatory, contractual requirements and litigation/lawsuits
 - damage to reputation of organization

Chapter 16

- cybersecurity is the protection of data assets from unauthorized electronic access or exploitation
- prevent, detect, respond
- effective oversight of cybersecurity is essential to company's oversight of risk management
- two core components:
 - compliance
 - controls

Chapter 16

- **compliance: company's program for ensuring adherence to cybersecurity policies, laws, regulations**
- controls: company's systems and processes for protecting data infrastructure and incident response
- **regulators' views on 'reasonable' cybersecurity are changing all the time**
- key inquiry revolves around value of each data asset
- has the organization adopted sufficient processes to inventory and value its various data assets?

Chapter 16

- time for board to play an oversight role is not when the data is put at risk
- board must build oversight into general strategy for overseeing risk management
- determine risk appetite
- board must be informed how risks are being managed
- board must be aware of compliance and controls
- lifecycle: identification, design and implementation, monitoring, evaluation, reporting and reassessment

Chapter 16

- extend enterprise-wide approach to compliance risk management system to company's entire ecosystem and third parties
- ensure independence of compliance team from company's IT and business units
- ensure ability to test compliance
- make cybersecurity compliance a priority
- **can't only focus on prevention and detection but response and remediation as well**

Chapter 16

- detection includes analysis of operational data and anomaly detection – logging, monitoring, and testing data moving in and out
- remediation includes incident response plans, exercises, measures to quickly restore from backups; recommend appointment of permanent incident response team including senior management, legal, compliance, vendor, PR, investor relations,

Chapter 16

- prioritize training of employees at a minimum annually on cybersecurity threats
- only takes one employee mistake to expose sensitive data
- cybersecurity controls must be appropriately funded
- common problem is disconnect between policies and operations and failure of board to notice
- should have appropriate metrics, reporting

Chapter 16

- **must recognize data as a valuable business asset**
- cybersecurity resources should be enterprise-wide
- human element is the weakest link in an otherwise solid data security program
- board should be apprised of data security incidents and emerging data risks

Chapter 17

- two important risk categories:
 - disputes
 - regulatory investigations
- may lead to bankruptcy
- difficult to quantify regulatory investigation risk
- “businesses end up attempting to comply with the strictest regime in which they operate”
- cybersecurity will increasingly impact contract

Chapter 17

- contract negotiation
- **critical to have flow down provisions with suppliers
(security requirements passed down to contracts)**
- liability/indemnity – cybersecurity creates risk
- contracts contain liability clauses but do not explicitly address cybersecurity matters
- data security and notification
- many businesses seek to keep breaches out of the press –
creates tension with notification provisions

Chapter 17

- data ownership/data processing
 - different roles
- **insurance companies may not pay if organizations cannot show they followed policies, laws, regulations, acceptable cyber hygiene**
- contractual counterparties
- notification provisions have an abbreviated time frame for notification
- in the wake of a breach security will come under



Chapter 17

- many intrusions lead to lawsuits by customers
- need to resume normal operations can pressure victim to agree to settlement
- may be class actions
- interconnected society spreads the effects
- insurance companies offering cyber policies
- federal regulators, industry regulators, most require 'reasonable security'

Chapter 17

- most standards are voluntary for private entities
- SEC has stated that materiality analysis for data breaches is the same as for other risk factors
- registrants should disclose the risk of cyber incidents
- California was the first to have breach notification law

Chapter 18

- in a data breach organizations likely to face different forms of legal and regulatory exposure – class action, shareholder, regulatory, forensic costs, individual notifications, credit monitoring, call centre services, public relations, event management
- business loss and day to day disruption
- **cyber insurance can play a role in organization's overall protection**

Chapter 18

- SEC issued guidance that companies should review on an ongoing basis the adequacy of their disclosure relating to cybersecurity risks and cyber incidents ... in the wake of more frequent and severe cyber incidents
- whether company has obtained cyber insurance, the amount
- **difficulties making claims against cyber insurance**
- **organizations may not pay if can show organization did not take necessary steps to protect**

Chapter 18

- emerging markets
 - first-party losses involving physical asset damage
 - third-party bodily injury
 - reputational injury resulting from public perception
- various liability, third party coverages – privacy, network security, regulatory, PCI, media
- first party coverages – crisis, network, contingent network, digital assets, extortion

Chapter 18

- cyber insurance market highly competitive and policies highly negotiable
- tips for cyber insurance:
 - adopt a team approach, understand risk profile and tolerance, ask the right questions, pay attention to the application, beware the fine print
- **failure to follow minimum required practices – void coverage if insured fails to continuously**

Chapter 18

- “they promised to protect us from a cyber breach if we paid the insurance premium – we paid the premium – they broke their promise”

Chapter 19

- responsibility on businesses to protect consumer info
- different from other crimes where the business is considered the victim, with cyber attacks the customers of the business are seen as the victim
- no organization is immune from cyber attacks
- **impenetrable data security is not possible**
- “the media and public vilify and hold businesses responsible for failing to do what experts

agree cannot be done”

Chapter 19

- consumer demand organizations safeguard their privacy and protect info
- consumers are impatient when security measures slow services or degrade usability
- businesses must maintain compliance with variety of laws, regulations, guidelines
- FTC is considered the most active agency in the world in enforcing data privacy and security

Chapter 19

- FTC can choose to investigate when it believes the organization is doing a poor job protecting consumers' information
- **know what info you have and who has access to it**
- **keep only info needed to conduct business**
- **protect info in your control**
- **dispose of info that is no longer needed**
- **prepare plan for responding to security incidents**

Chapter 19

- failure to place consumer protecting and cybersecurity at the top of priority list may land organization in regulatory body crosshairs
- risk management and oversight
- threat intelligence – track cyber activities, vulnerabilities, threats
- cybersecurity controls
- external dependency management
- cyber incident management and resilience

Chapter 19

- discussion on GLBA, HIPAA
- organizations must build privacy and security into systems, processes and services from ground up and top down
- **education and training for all employees should start on day one**
- technology is continually evolving so cybersecurity does as well

Chapter 20

- theft of IP is the ‘greatest transfer of wealth in human history’
- estimated at \$300 billion a year
- “national industrial policy goals in China encourage IP theft and a number of Chinese in business and government entities are engaged in this practice”
- **US used indictment to send two strong signals**
 - 1) we are aware of the behavior
 - 2) we will expose the misconduct to the world

Chapter 20

- companies should focus on taking immediate reasonable steps to defend their IP assets
- **4 categories of IP**
 - patents
 - trademarks
 - copyrights
 - trade secrets
- trade secrets are the only one to maintain
their value



Chapter 20

- companies should implement access controls on crown jewel data
- **nobody should need access to all trade secrets**
- distribute info so that no single cybersecurity breach exposes enough of a trade secret to allow the attacker to obtain the full set of information
- negative information is valuable information about what does NOT work

Chapter 20

- companies should flag and investigate instances and activity of high volume or suspicious data transfers – not just watch for unauthorized access
- **companies should mark their files**
- **sample techniques are: meta-tagging, beaconing, and watermarking**
- can determine if information has left the network
- software can allow only authorized users to open files with valuable information

Chapter 20

- **key to ensure have an incident response plan that is tested**
- trade secrets can be stolen to use, sell, and profit from them
- misappropriation of trade secrets, computer fraud and abuse act, call the feds
- **pros and cons before bringing civil litigation or involving law enforcement**



University
of Victoria

(eg. it is a good idea to involve
law enforcement every time = FALSE)

Chapter 21

- when you buy a company you buy their data (and the risks)
- **organizations need to know what info and systems are most important (crown jewels)**
 - where is sensitive info stored
 - how is it protected in transit, at rest, and in motion
- most concerning threats to info, networks, systems
- have there been incidents? what is the security budget? what are the recovery plans?

Chapter 21

- should have integrated cyber risk awareness and mitigation and comprehensive security management program
- **security program will not be effective if it is a silo inside IT or information security**
- is there a designated person with responsibility? who do they report to?
- describe board oversight

Chapter 21

- does company have legal counsel advising on compliance? internal or external?
- how does company educate and train
- how can employees/public report vulnerabilities/breaches/irregularities
- what is the plan to recover if systems are unavailable
- expenses due to incident include costs to investigate/contain/remediate, liability to banks, card reissuance, expense of legal/technical/comms

Chapter 21

- reference to Sony Attack
 - attribution to North Korea
- are there former employees who had access to critical infrastructure who have left to competitors?
- what agreements are in place to protect proprietary information
- have you suffered thefts of data? has network suffered an intrusion? did you retain outside experts?

Chapter 21

- what is known about attackers and attack vector?
- what data do you suspect or know were taken?
- how long between first known intrusion and discovery?
- do you know if intruder attempted or made fraudulent or competitive use of exfiltrated data?
- during past 3 years have you had an interruption of your system for any unplanned reason?

Chapter 21

- controls
- **pre-employment screening, background/reference checks**
- workforce education on warning signs
- internal network security measures (eg. website monitoring, cloud storage, USB drives)
- automated monitoring of web, peer to peer, darkweb for leaked data

Chapter 21

- has the company evaluated exposure to attacks?
- what measures are in place to defend?
- how would it know if an attack was occurring?
- have any attacks occurred?
- **consider cyber insurance**

Chapter 22

- technology, software, hardware, and physical and social networks are embedded everywhere today
- next wave of global hyper connectedness
- every business today is a technology business
- every society is increasingly a technology society
- have to create acceptable 'rules of the road' in cyberspace
- pace of change is accelerating

Chapter 22

- three areas companies and leaders can help
 - rules of the road, cyber laws globally and security and privacy
- cyber is a top issue for US, EU member states, China, India, Russia, Brazil, Australia, Japan
- **US has said that cyber is the number one national security threat to the US**
- in national security cyber is both an offensive and defensive issue

Chapter 22

- no company wants to have its operations, brand, or competitive advantage undermined or destroyed
- cyber is the fifth fighting domain along with land, sea, air, and space and the only one owned by private companies
- what cyber activity is an act of war? espionage? vandalism? what is acceptable on a bank, stock exchange, energy, transportation, electric, or life

Chapter 22

- the future of the global interoperable open secure network is at stake
- **compliance does not equal security**
- driving to real security is the goal
- different laws in different jurisdictions
- goal is to do security and privacy
- cybersecurity is a global issue
- need common ground on what's okay and



Chapter 23

- what is secure enough
- how do we manage/minimize third-party liability
- insurance is an option but obtaining a comprehensive policy is very expensive and coverage is uncertain
- [[nothing on SAFETY Act or US legislation will be tested]]

Chapter 24

- insider threat
- negligent and malicious insiders were the cause of 61% of security breaches
- reduce the risk of insider threats – screening employees to exit interviews, managing remote work, securing mobile devices, providing effective training
- **importance of background checks**
- recommend recurring checks or risk alerts

Chapter 24

- continuous monitoring
- safeguarding electronic data
- access control lists based on need-to-know
- roles and responsibilities
- protecting log-in credentials
- phishing emails
- screen security and shoulder surfers
- mobile device security, encryption, password protection, auto log out, remote wipe

Chapter 24

- remote work security
- unsecured WiFi
- VPN
- secure storage
- no storage in personal online accounts
- **clean desk policy (desk is free of sensitive material)**
- secure printers, scanners, fax machines
- secure disposal of paper documents

Chapter 24

- private conversations in private places
- **alert on idiosyncrasies in employee behaviours – eg. suddenly downloading large amounts of info**
- user based analytics
- data loss prevention
- **3 needs to manage confidential info with employees:**
 1. confidentiality agreements
 2. educating employees on information security
 3. modify exit interview process to address

Chapter 24

- recover devices
- arrange for remote wiping if necessary
- confirm employee hasn't stored sensitive data
- making human resources and legal valued members of info security team organizations can enhance security effectiveness
- HR and legal can enhance organization's security
- involvement in new hires, training, service providers

Chapter 25

- always on connectivity transforming how we live, work and do business
- game-changing technology, more efficient workers, new revenue streams, stronger customer relationships
- **technology is a core business enabler**
- **technology must be protected**
- hyper-connectivity requires new strategies with broader view of risk

Chapter 25

- cybersecurity strategy starts with placing it in the context of your business
- take the view of the CEO and board
 - 1) how does cybersecurity enable the business?
 - 2) how does cyber risk affect the business?
- focus on competitive advantage
- **if done right cybersecurity helps drive a consistent high quality customer experience**

Chapter 25

- important to know what must be protected
 - enterprise IT
 - supply chain
 - product/service development
 - customer experience
- external influencers (regulators, law enforcement, media, competitors, customers)
- requires enterprise wide collaboration

Chapter 25

- requires multidisciplinary team reflecting scale and complexity of business
- start with vision, understand risk, identify controls, and organizational capacity
- prioritize crown jewels
- set a vision, sharpen priorities, build a team, enhance controls, monitor the threat, plan for contingencies, transform the culture

Chapter 25

- build momentum with quick wins while investing in long term capability development
- use risk framework to assess where to apply controls
- **utilize drills, exercises, assessments to test and improve**
- don't adopt standards blindly
- assess priorities, set maturity target, build a roadmap
- have a mixture of short, medium and long term goals

Chapter 25

- successful cyber strategies:
- **are driven from the top**
- **security by design**
- **use business language**
- change agents, thought leaders to spread security vision
- security is embedded
- enterprise embraces it – do security without

Chapter 26

- defense in depth
- moat and castle defense
- need better incident response capability to detect, contain, remediate
- prevention is critical but can't just focus on that, must be able to respond and recover
- need a comprehensive, integrated approach to security

Chapter 26

- **guaranteeing there will be no security incidents is impossible**
- goal is to ensure security efforts coordinated efficiently
- threat defense, threat intelligence, red team
- tiered SOC structure – Tier 1, Tier 2, Tier 3
- Tier 1: classify severity of event and correlate with history
- escalate if necessary to Tier 2 and 3

Chapter 26

- **alert fatigue refers to the condition of analysts when they are exposed to so many alerts they are overwhelmed and unable to action any**
- **more technology, tools, and threat feeds do not enable your SOC to operate more efficiently**
- **enable detection, identify threats, mitigate threats**
- **modern day threats necessitate that SOC's operate 24/7, 365 days a year with well thought shift schedules and defined roles**

Chapter 26

- organizations must carefully consider new tech and tools will impact analysts workflow and ability to detect and respond to threats while also necessary processes and procedures
- true meaning and value of threat intelligence has become clouded
- **a lot of false threat intelligence claims out there**
- **true threat intelligence is incredibly powerful**

Chapter 26

- **actionable threat intelligence is the goal**
- actionable threat intelligence is created when large volumes of data and information are analyzed why specific pieces of information are relevant to your organization
- will your organization be ready when an attack comes?
- **one way of assessing is to attack it through exercises, drills, tests, coordinated Red Team exercises**

Chapter 26

- what types of threats does your SOC observe?
- what types do they not see?
- are there gaps in detection? what do they mitigate well and worth testing?
- maintain healthy relationship between **red and blue teams**
- **mission is the same – protect the organization and improve security capabilities**

Chapter 26

- efforts to protect are diminished by easily exploitable vulnerabilities, unnecessary services, non-essential assets
- understand and prioritize your attack surface
- know your crown jewels

Chapter 27

- what are they really after?
- popularity of standards has increased and decreased
- identify assets, risk management, establish preventative, detective, corrective controls
- map controls to a framework and identify gaps/vulnerabilities
- after sensitive information like credit cards
- significant amounts will be a bigger target

Chapter 27

- do you know where sensitive data is?
- is the access tightly controlled?
- is the data encrypted to thwart attacks?
- intellectual property, personally identifiable information, and other confidential information is at risk
- target of activism? (eg. anti capitalism, pharma, farming, etc)

Chapter 27

- reference to DDoS and defacement
- do we have controls against DDoS? what would be the impact of a DDoS attack?
- do you provide critical infrastructure?
- another target for attackers
- do employees understand their role in protecting?
- do you have a strong incident response capability?
- do you have sufficient controls? eg. two-factor

Chapter 27

- do you have a role that is responsible for cybersecurity?
- are only required services exposed on the internet?
- are PCs and email servers protected?
- do corporate controls block malicious websites and infected emails, links?
- **reference to ransomware**
- **need for offline backups that are tested**
- **offline backups and security awareness are effective controls along with application whitelisting and quarantine/sandboxing (exploding malware samples before executing)**

Chapter 28

- keeping up with attackers' evolving techniques is difficult
- increasing frequency and sophistication of attacks
- some vulnerabilities are known only to the attacker (zero days)
- others are known to general public but not fixed by software vendor
- one problem is sheer number of disjointed

Chapter 28

- organizations can't hire their way out of this problem
- organizations should consider next-generation technology
- customers more and more reliant on internet and networks for business and access to services
- **zero trust: security posture focuses on only allowing legitimate users and applications as opposed to trying to block everyone**

Chapter 28

- blocking techniques attackers might use to evade detection and establish command and control
- prevent installation of malware
- closely monitoring and controlling traffic
- **tools, tactics, and procedures – TTP**
- **C&C – command and control – also called C2**
- advanced persistent threats (APT) – goal is to gain access, maintain persistence, go undetected, trickle out the data

Chapter 28

- references to reconnaissance, weaponization and delivery, spearphishing, waterholing, exploitation, zero days, installation, remote access tools (RATs)
- focus on proactive rather than just reactive
- must force the attackers to invest more and more so their attack becomes unprofitable
- reduce attack surface, allow only authorized traffic, segment your network, secure the endpoints,

Chapter 28

- **security awareness is often said to have the greatest ROI (return on investment)**
- “if organizations continue to view investments in cybersecurity simply as cost centres to be solved by bolting on legacy technology we will all continue to suffer the consequences”

Chapter 29

- organizations depend on other organizations to operate – presently it is common for these organizations to have ‘always-on’ connections or other trusted access between companies
- these other organizations can be used to compromise your organization
- **that’s why it’s important to understand and secure your supply chain**

Chapter 29

- you inherit the risks of your suppliers
- especially if you don't test them
- complying with standards and guidelines is not enough for securing all the factors required
- can help identify issues and set minimum level
- don't just focus on a standard, look at your program with a maturity lens
- **special considerations for your organization**

may mean 'one size fits all doesn't work'

Chapter 29

- most companies do not have the appetite or budget for wholesale drastic changes
- conduct a maturity assessment and build a roadmap
- identify key risks throughout supply chain
- decompress your key product lines
- supply chain cybersecurity may be a differentiator

Chapter 30

- reference to Target
- organizations may need to share sensitive information of their customers or others with third parties
- inherent risk in third-party services
- new avenues of attack against company data
- in Target case attackers came in through their HVAC supplier and targeted Target point-of-sale systems
- cost of breach was \$150 million and included

Chapter 30

- reference to several US standards
- breaches of personal data, proprietary data, financial harm, confidential info
- reference to Dairy Queen and Heartbleed issues
- 3 elements are common to all 3rd party risk management: due diligence prior, contractual commitments and legal risk management, ongoing monitoring and oversight

Chapter 30

- interesting references to “whether and how often the vendor has experienced incidents, the severity and quality of vendor response; whether the vendor maintains security policies, organizational considerations, etc” – almost foreshadowing the Marriott breach that was discovered only when they went to do a merger
- don’t forget physical security, backup and recovery, change controls and others

Chapter 30

- “a third party vendor should be fully responsible for any liability for data breaches that occur while the data are under the vendor’s control”
- need to make periodic checks
- trust but verify
- vendor contract should also contain notification and remediation provisions if vendor becomes aware of deficiencies

Chapter 30

- party of the agreement may seek right to terminate if security is violated
- may also seek penalties/damages
- maintain diligence, contractual terms, and continued monitoring and oversight as parts of a comprehensive cybersecurity program managing third-party relationships
- also have standardized processes and documentation

Chapter 31

- need to take the insider threat seriously
- **people are the most consequential part of security**
- reference to Snowden
- vast amount of vital business and personal data online
- migration of data outside the perimeter
- increase in marketability of confidential data
- **insider is the person who the enterprise has trusted to access and operate with company data**

Chapter 31

- reference to Home Depot and attackers entering using vendor's legitimate access credentials
- **without trustworthy insiders the organization cannot function**
- two types of insiders:
 - 1) malicious insider
 - 2) unwitting insider

Chapter 31

- malicious insider may become one due to anger as a result of conflicts or disputes, fear of termination, dissatisfaction with workplace, ideology, or financial need
- unwitting insider includes those who have lax attitude about security
- phishing and social engineering very common
- more than 75% of malware installs were the result of users clicking on attachments or links

Chapter 31

- **increase in insider threat events**
 - **most organizations don't have adequate controls**
 - **may be more difficult to detect**
 - **often only detected after individuals leave**
- **most handled internally without legal or police**
- **take the insider threat seriously**
- **technology itself is not the answer**

Chapter 31

- establish threat aware culture
- strong security awareness
- build a multi-disciplinary program
- creation and oversight of policies
- personnel reliability processes
- decision-making authority
- building and operating security controls
- monitoring/detecting insiders

Chapter 31

- **with legitimate authorization to access company and information resources an insider can do significant harm to the organization**

Chapter 32

- 7.4 billion devices connected to the IoT
- by 2020 will be 26 to 75 billion
- IoT brings addition to responsibilities of cybersecurity
 - safety
- convergence between physical and logical
- lack of recognition of seriousness of the threat leads to lack of security sufficient to defend
- IOT creates issues with privacy

Chapter 32

- data we give away on the internet, on social media is often sorted for resale to advertisers and marketers
- evolving technology landscape is a big concern
- **70% of IoT devices contain security vulnerabilities**
- **if it's connected to the internet it can be hacked**
- **everything is being connected to the internet**
- **therefore everything can be hacked**
- we will ask why things aren't connected to the

Chapter 33

- decision to call law enforcement can be difficult
- there may be reasons to call LE and reasons not to
- perception of loss of confidentiality, loss of control
- *law enforcement understands company concerns*
- conflicting goals?
- agencies have evolved to protect public safety in a way that does not cause further harm?

Chapter 33

- benefits to working with law enforcement
 - law enforcement can compel 3rd parties to provide information
 - can work with foreign counterparts
 - early reporting looks good to investigators/auditors later
 - law enforcement may delay reporting to further investigation
 - prosecution may prevent attacker from doing more harm
 - information may protect other victims

Chapter 33

- US law enforcement works cooperatively and discreetly with victims
- they try to minimize disruption
- can protect sensitive information from disclosure
- ensure visibility (is it still ongoing? how do you know?) and logging in place (who did what when)
- identify who will work with law enforcement

Chapter 33

- ensure you involve legal
- establish relationships with law enforcement in advance
- what organizations are out there?
- work together to ensure there is “no wrong door” for victims
- for incidents, did you find it yourself or were you notified by a third party?

Chapter 33

- difficult to track down attackers
- difficult to hold them responsible
- “hacking back” is often illegal in the US
 - many intrusions are perpetrated from infected machines so hacking back may affect a victim’s machine
- prepare/plan in advance

Chapter 33

- decision to call law enforcement can be difficult
- there are reasons to call LE and reasons not to
- perception of loss of confidentiality, loss of control
- *law enforcement understands company concerns*
- conflicting goals?
- agencies have evolved to protect public safety in a way that does not cause further harm?

Chapter 33

- benefits to working with law enforcement
 - law enforcement can compel 3rd parties to provide information
 - can work with foreign counterparts
 - early reporting looks good to investigators/auditors later
 - law enforcement may delay reporting to further investigation
 - prosecution may prevent attacker from doing more harm
 - information may protect other victims

Chapter 33

- US law enforcement works cooperatively and discreetly with victims
- they try to minimize disruption
- can protect sensitive information from disclosure
- ensure visibility (is it still ongoing? how do you know?) and logging in place (who did what when)
- identify who will work with law enforcement

Chapter 33

- ensure you involve legal
- establish relationships with law enforcement in advance
- what organizations are out there?
- work together to ensure there is “no wrong door” for victims
- for incidents, did you find it yourself or were you notified by a third party?



Chapter 33

- difficult to track down attackers
- difficult to hold them responsible
- “hacking back” is often illegal in the US
 - many intrusions are perpetrated from infected machines so hacking back may affect a victim’s machine
- prepare/plan in advance

Chapter 34

- planning and preparation are key
- what do you do first during a major breach?
- CISO needs to be empowered by the C-suite
 - connect on security trends regularly
- everyone has a role to play
- challenging to stay on top of cyber risks
- prepare, detect, respond, remediate

Chapter 34

- good cyber incident management plan considers the whole enterprise
- plans must be tested and updated frequently
- ensure staff have the proper skills
- consider external partnerships
- support plan with runbooks
- importance of asset management, detection capability, exercises

Chapter 34

- red team: group whose purpose is to simulate the cyberadversary
- engage third party to validate plan
- cybersecurity landscape changes every day
- engage communications proactively and develop messaging to be used

Chapter 35

- 67% of board members have some to no knowledge of cybersecurity
- different threat actors have different motivations, access to resources, level of sophistication
- Nortel example

Chapter 35

- **Questions to ask about risk**
 - Who are our most likely intruders?
 - What is the biggest weakness in our IT systems?
 - What are our most critical and valued data assets? Where are they located?
 - Do we consider external and internal threats when planning cybersecurity programs?
 - Do our vendor partners have adequate security measures? Do we have sufficient contractual clauses regarding such security?
 - What are best practices for cybersecurity? Where do our practices differ?
 - Have we created an incident response plan?

Chapter 35

- IOC: indicator of compromise
- cybersecurity poses a serious risk
- boards that fail to manage cybersecurity risk will leave the organization exposed to significant risk
- board members do not need to be cyber experts

Chapter 36

- value of engaging independent and impartial breach response firm
- insurance example
- important to manage communications effectively
- is there information to report? is disclosure required? has the incident been leaked?

Chapter 36

- will the organization detect the breach? probably not
- assume compromise
- getting the right people involved is essential

Chapter 37

- cybersecurity attacks are getting worse
- what can be done to minimize the damage
- CISOs have to translate the information into business terms
- effective command and control in times of crisis is critical
- slow response and uncoordinated can provide attackers the window they need

Chapter 37

- do drills and implement lessons-learned
- have a team dedicated, virtual or on-retainer
- involve an external party
- consider external counsel, forensics
- even if issue may not go to court pretend as if it will
- ensure you do a debrief following the attack

Chapter 37

- no organization is immune to cyber attacks
- organizations must have a team
- ensure right parties are briefed ahead of incident
- conduct exercises
- build in lessons learned

Chapter 38

- ensure you have a plan
- test the plan
- have a team
- test the team
- identify lead for the team
- categorize the incident
- identify third parties to assist

Chapter 38

- create a time-line of events
- comply with legal obligations
- preparation, identification, assessment, communication, containment, eradication, recovery, post-incident
- notification
- relevant laws, regulations – PCI reference

Chapter 39

- data breach can substantially diminish stock value
- cost is \$3.72 million on average
- preserve company's credibility
- maintain control of communications
- provide confirmed facts
- coordinate communications/legal
- prepare for negative scenarios

Chapter 39

- cybersecurity is the number one fear keeping directors up at night
- communications is critical
- preparation and planning are critical
- develop the plan
- identify the team and lead
- practice

Chapter 40

- two kinds of companies, those that know they have been hacked and those that don't know yet
- operate as if the bad guys are already inside
- **no vendor has the silver bullet to solve security**
- **cyber insurance may lower the risk impact curve overall***
- benchmarking is still useful
- focus on minimizing cyber risk

Chapter 41

- many CISOs view risk avoidance as extremely challenging
- need to mitigate and build enterprise resilience
- reference to APTs
- heightened interest by board
- increased regulatory risk
- financial penalties
- insider risk

Chapter 41

- **security is not equal to compliance**
- insurers do not address all enterprise assets at risk
- insurable costs range from data breach response costs to defence costs and damages
- some claim to insure against reputation and brand
- prediction that insurers will partner with security industry to use tools that predict and monitor the threat

Chapter 41

- cyber insurance market is only 15 years old
- noted some items to negotiate
- cyber insurance has larger role than just reimbursing costs
- increased regulator and shareholder scrutiny

Chapter 42

- nearly all cyber vulnerabilities begin and end with some kind of human error
- despite millions spent on security technology weakness often comes down to humans
- cybercrime most prevalent economic crime
- number of attacks increasing
- impacts and costs of attacks are high
- it is a strategy problem, human problem,

Chapter 42

- internal weaknesses are a problem
- data leaks by employees are a problem – intentionally and unintentionally
- job of educating employees is never finished
- no substitute for sound well understood culture of responsibility and awareness around security
- unhappy or untrained employees can be a company's biggest threat – if trained can be biggest



Chapter 43

- delivering results is a key metric of success for any leader
- leaders need the right information at the right time
- must be understood and actionable
- identify stakeholders
- C level executives, board of directors, audit, many others

Chapter 43

- cybersecurity committee can review strategic direction and planned initiatives, discuss major milestones for security initiatives in progress
- assess impact of program changes
- discuss lessons learned
- identify areas of conflict or resource constraints
- discuss impacts from/to larger industry
- stakeholders want facts and reassurance

Chapter 43

- **tell the security story throughout the organization in clear, concise, targeted communications**
- publish newsletter, intranet presence, celebrate successes, provide platforms for cyber champion recognition
- track/measure/report effectiveness of communications
- **don't pass up the opportunity to build a champion**

Chapter 44

- **demand for professionals outweighs the supply**
- broader skillset desired – communication, change management, leadership
- rethink approach, develop alternative talent management strategies, empower leadership, connect your organization, invest in cyber human capital
- major breach poses major problems
- ensure have the proper culture to

Chapter 44

- agile, multifunctional, inquisitive
- understand work preferences
- reward employees for forward thinking
- CISOs should have a seat at the table
- CISO must have strategy and tactical, business and technical
- cybersecurity should be seen as a central business unit that informs other business units

Chapter 44

- **it doesn't matter how strong your security posture is for individual departments, if one is vulnerable the whole organization is at risk**

Chapter 45

- **no foolproof way of preventing breaches**
- estimated close to $\frac{3}{4}$ breaches go undetected
- can't afford to become complacent
- if not a victim yet you may have been smart but most likely lucky
- assume it's only a matter of time
- short amount of time cyber has gone from IT dept to being discussed regularly at the board

Chapter 45

- until cybersecurity is on balance sheet terms it's not going to be fully embraced by the board
- cybersecurity is a critical risk
- companies depend on a functioning internet
- is cyber risk accounted for in our planning?
- what is the process for evaluating security and measuring liabilities?
- do we have directors with relevant expertise?

Chapter 45

- have we identified executive ownership of the issue?
what will we do in the event of a breach?
- directors should be kept abreast of main cyber risks
- cyber has expanded well beyond IT
- no company in the US should forego buying cyber insurance to protect against the real risk of major cyber attack and the costs associated

Chapter 45

- baseline for board:
 - security strategy
 - policy and budget review
 - security leadership
 - incident response plan
 - ongoing assessment
 - internal education

Chapter 46

- role of CISO has changed dramatically
- full strategic partner
- must have wide variety of skills
- should have technical understanding
- results orientation, strategic orientation, transformational leadership, relationship management, team leadership
- four elements: curiosity, insight, engagement, determination

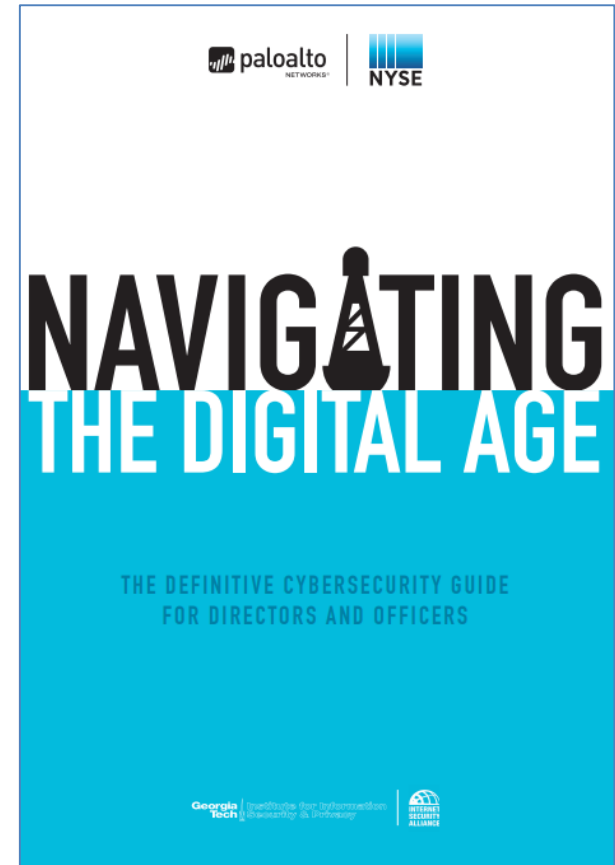
Textbook

- All notes generated from:

Navigating the Digital Age

- Link

- https://www.securityroundtable.org/wp-content/uploads/2015/09/Cybersecurity-9780996498203-no_marks.pdf





University
of Victoria

