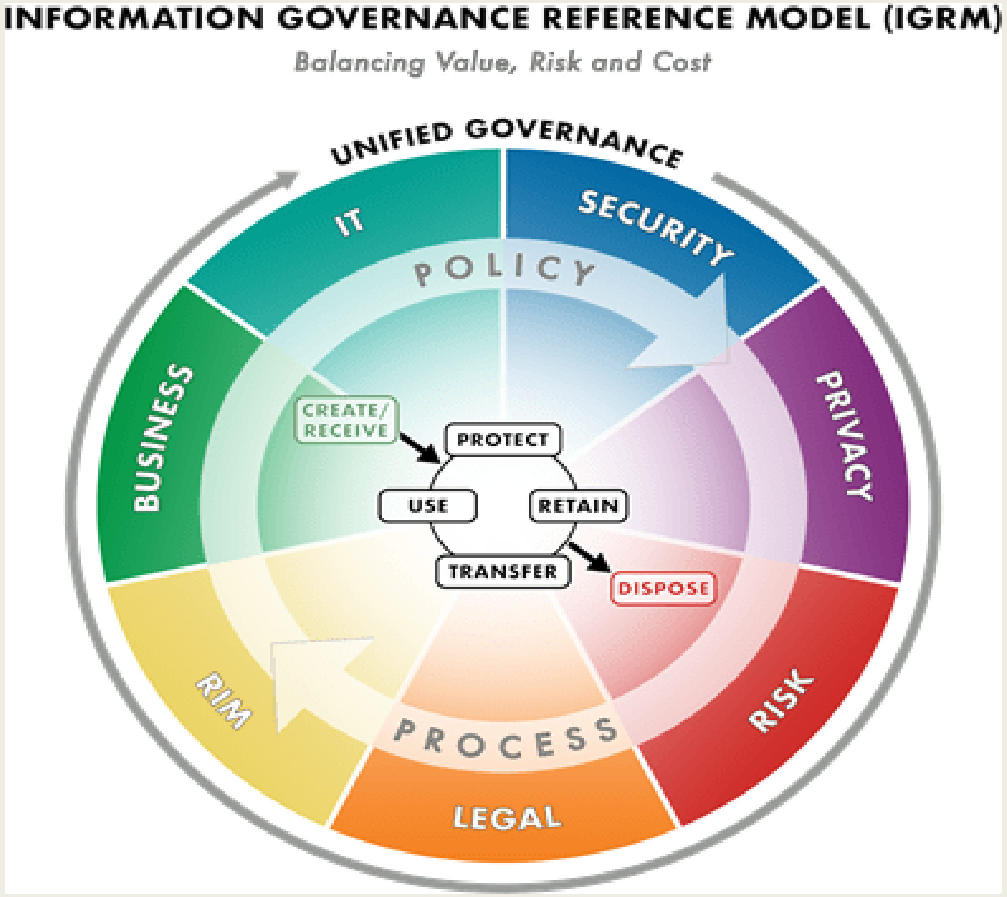
CYBER RISK

With Nicholas Fonseca, MBA, BSB/M, CIP, CTAJ(TM)

Bringing Together RiM and Cyber Concepts

IGRM (edrm.net)
Leveraging the model for Collaboration



Cyber Training ?
Let’s discuss! ☺

DAD'S TEACHING ME ABOUT CYBERSECURITY.
Rothstein/MORGAN 2023
CYBERSECURITY VENTURES
CYBERSECURITYVENTURES.COM

Welcome!

Cyber Risk Defined & What is it?

- Any risk of financial loss, disruption of business or damage to an organization’s reputation due to the failure of its information technology systems (Insurance Institute of Canada, 2020)
- Unintentional or accidental security breaches such as losing a memory stick or a laptop or falling victim to social engineering attacks.
- Deliberate and unauthorized breaches od security to access information systems for the purpose of destruction, espionage, extortion or embarrassment of an organization, such as ransomware to lock businesses from accessing their data
- Operational IT risks – Failing to install firewalls, failure to keep security software and software up to date, lack of proper security

Cyber Crime

- Cyber Crime is a criminal offence committed through a computer or the internet that causes loss or damage to the victim’s computer system, network or data, denies access to data denies access to data or service or enables further related crimes such as extortion or the resale of stolen data. (Insurance Institute of Canada, 2020)

The Criminal Code of Canada has been amended to include the following as cyber criminal activity

- Using a computer without authorization
- Making mischief in relation to data
- Possession of a device to obtain telecommunication facility or service without authorization
- Stealing telecommunication service

Examples of Cyber Attacks

- **Phishing and social-engineering-based attacks.** Attackers trick legitimate users with proper access credentials into taking action that opens the door for unauthorized users, allowing them to transfer information and data out (data exfiltration).
- **Internet-facing service risks (including cloud services).** These threats relate to the failure of enterprises, partners and vendors to adequately secure cloud services or other internet-facing services (for example, configuration management failure) from known threats.
- **Password-related account compromises.** Unauthorized users deploy software or other hacking techniques to identify common and reused passwords they can exploit to gain access to confidential systems, data or assets.

(Gartner Research , 2023)

Examples of Cyber Attacks

- **Network-related and man-in-the-middle attacks.**
  Attackers may be able to eavesdrop on unsecured network traffic or redirect or interrupt traffic as a result of failure to encrypt messages within and outside an organization’s firewall.
- **Supply chain attacks.**
  Partners, vendors or other third-party assets or systems (or code) become compromised, creating a vector to attack or exfiltrate information from enterprise systems.
- **Denial-of-service attacks (DoS).**
  Attackers overwhelm enterprise systems and cause a temporary shutdown or slowdown. Distributed DoS (DDoS) attacks also flood systems, but by using a network of devices. (Also see “What is a DDos attack?”)
- **Ransomware.**
  This malicious software infects an organization’s systems and restricts access to encrypted data or systems until a ransom is paid to the perpetrator. Some attackers threaten to release data if the ransom isn’t paid.

(Gartner Research, 2023)

- Security & Risk Strategy

Cyber Event Expenses (resulting from exposures)

- Privacy Breach resulting in Personal Identity Theft (3rd party)
- Internet Media Liability (3rd party)
- Network Security Liability (3rd party)
- Technology Errors and Omissions Liability (3rd party)
- Event –Expenses (1st party)
- Extortion Expenses (1st party)
- Restoration Expenses (1st party)
- Regulatory Expenses (1st party)
- Business Interruption (1st party)

Cyber Incidents

- Colonial Pipeline
- SAS – Scandinavian Air
- Marriott
- The Running Room
- Equifax
- City of Atlanta
- Maersk
- LCBO
- Indigo
- Empire, Sobeys, IGA
- Bell
- Government of Canada
- And the list goes on……. Cyber attacks in Canada | KonBriefing.com

Records and Information Management

- Need to know what records and information you have and where it is
- How many records do you have?
- You need to protect your data, records and information
- Protect your records, information and data
- The Need for Policies
- Have a records information and data classification policy
- Follow your data, records and information classification policy
- Have a records, information and data retention schedule
- Follow your retention schedule
- Provide training to staff
- Have a clean desk and clean screen policies
- May need to have an understanding of key concepts and have a seat at the table

Risk Management & Enterprise Risk Management

- Risk Management (RM) – analyzing a risk to quantify the potential for losses in a specific in vestment and to decide what is the appropriate action to take (or whether not to take the risk)

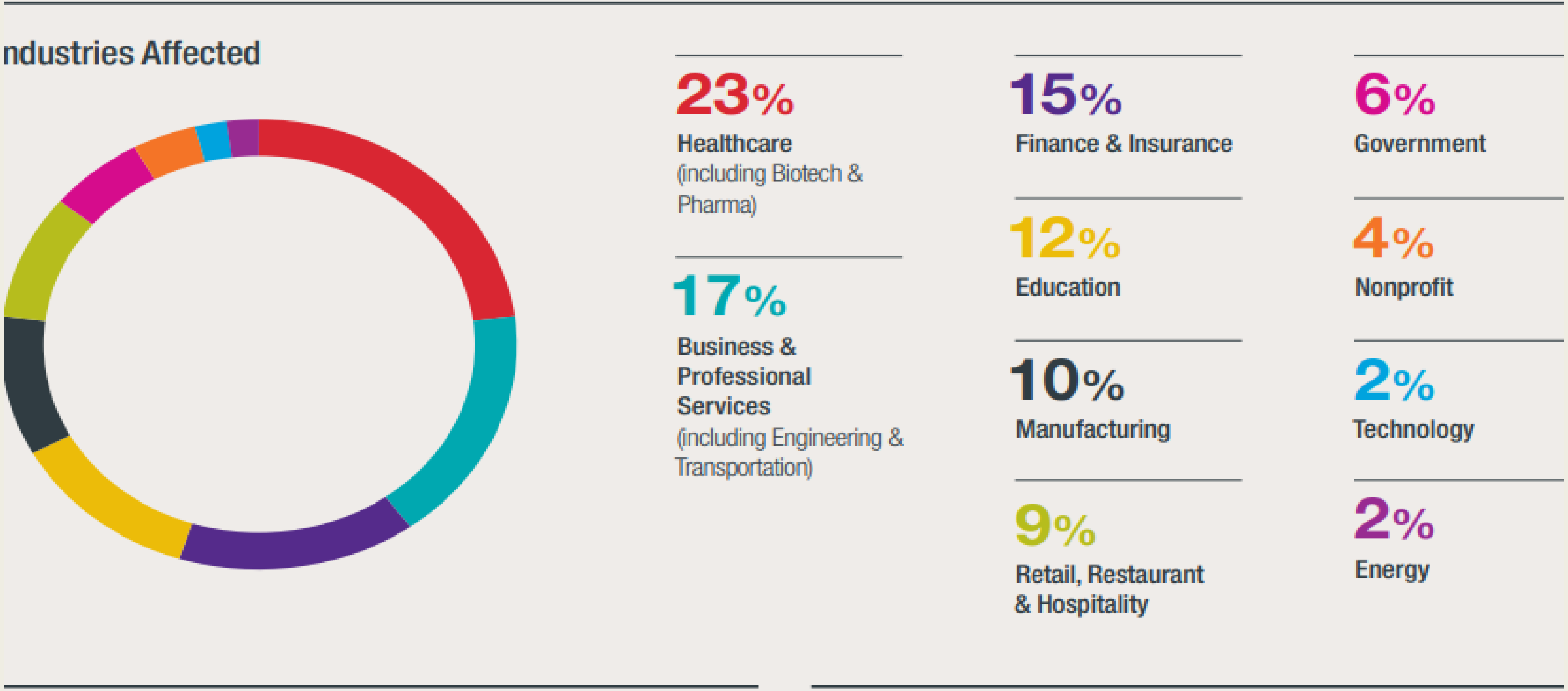
(Insurance Institute of Canada, 2020)

- Enterprise Risk Management (ERM) – An approach to managing all of an organization’s key business and opportunities with the intent of maximizing shareholder value. ……ERM is about avoiding (preventing), reducing and eliminating risks through the creation of risk management strategies. (Insurance Institute of Canada, 2020)
- ERM doesn’t always include cyber risk. It may be seen as an IT responsibility

Risk Management and ERM (Cont’d.)

- Risk management can include risk transfer.
- Insurance is one way of risk transfer
- Avoidance – is an option. A risk management technique whereby the risk of a loss- in this case due to a cyber attack – is prevented by not engaging in the activity that present the risk.
- Avoidance could likely mean missed economic opportunities
- Insurers want their policyholders to exercise good cyber risk management generally; not just through risk transfer
- Have a tested disaster recovery plan, business continuity plan and excellent cyber security plan

Cyber attacks impact……….(Baker Hostetler, 2022)



ndustries Affected

23% Healthcare (including Biotech & Pharma)

17% Business & Professional Services (including Engineering & Transportation)

15% Finance & Insurance

12% Education

10% Manufacturing

9% Retail, Restaurant & Hospitality

6% Government

4% Nonprofit

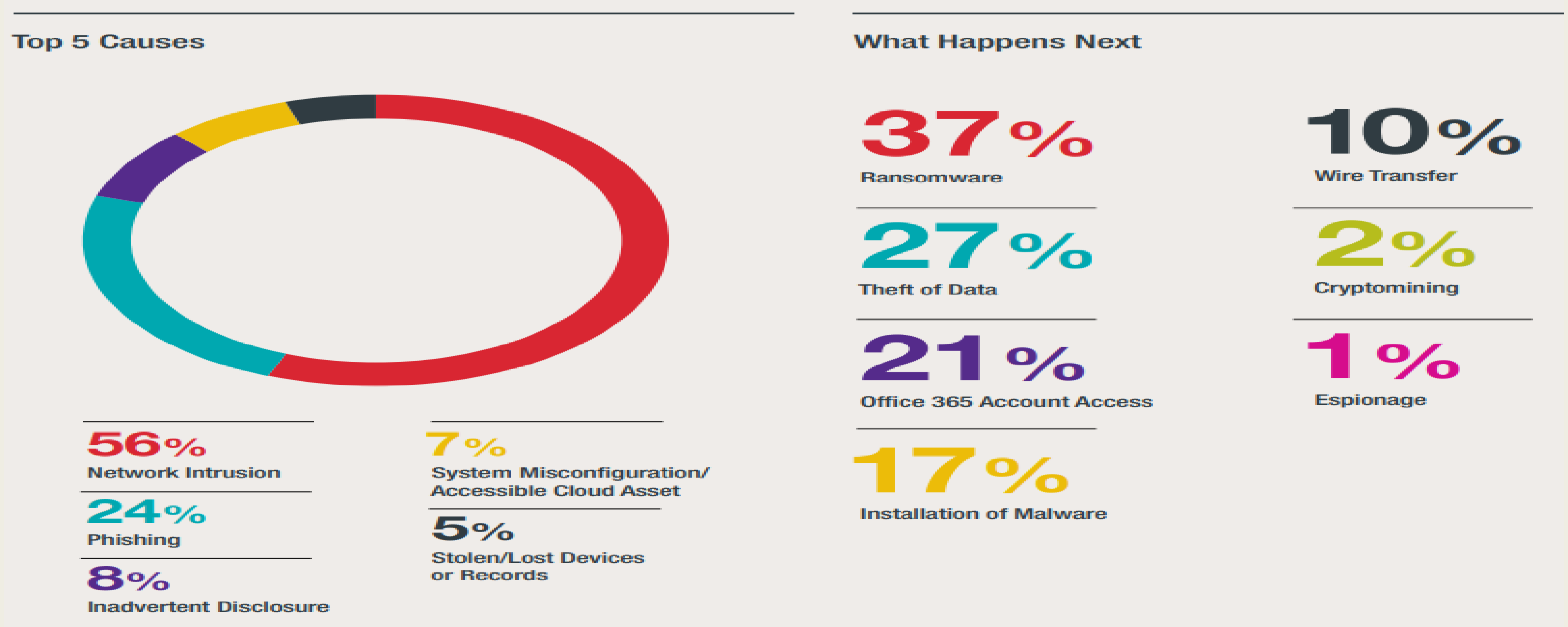
2% Technology

2% Energy

Baker Hostetler 2022 summarizes…….

- Ransomware remained the most prevalent and impactful type of data security incident. Investments in security enhancements and business continuity practices are making companies more resilient and less likely to choose to pay, driving down the average ransom payment amount. Threat actors continue to evolve tactics to increase extortion leverage, such as using publication countdown timers and contacting employees and customers directly to pressure the company to pay.
- The pandemic, technology strategy and business continuity advantages are driving increased use of cloud assets, which also changes the risk landscape and makes additional security measures, like asset management and access controls, increasingly important.
- E-crime continued, including a surge of wire fraud precipitated by gaining access to email accounts. There are concerns about e-crime actors supporting state entities as a result of the Russia/Ukraine war.

And more from Baker Hostetler……(2022)



Top 5 Causes

56% Network Intrusion

24% Phishing

8% Inadvertent Disclosure

7% System Misconfiguration/ Accessible Cloud Asset

5% Stolen/Lost Devices or Records

What Happens Next

37% Ransomware

27% Theft of Data

21% Office 365 Account Access

17% Installation of Malware

10% Wire Transfer

2% Cryptomining

1% Espionage

Cyber Risk is insurable OR is it?

- Insurance companies have relied on actuarial data to price policies or risk exposure
- Rating has been based on location of the exposure (risk-the subject of insurance)
- Policies were standardized to some degree (not so for Cyber risk and insurance)
- Cyber exposure is not subject to geographical boundaries
- Cyber attacks can be targeted to specific verticals
- Attacks can come from anywhere in the world
- Cyber attackers have there own software available as a service, Ie MaaS, Raas
- Cyber attackers may use server space on hidden servers to launch their attacks
- By 2025, it is estimate that cyber crime will cost 10.5 trillion annually (Cyber Ventures, 2023)

Cyber Insurers

Want to know…..

- There is a cyber disaster recovery plan for a cyber event
- There is a business continuity plan in place
- That the plans are relevant and tested
- Adequate cyber security controls are in place such as anti- virus software, firewalls, patches are up to date, removal of unused software,
- Compliance with standards
- Compliance with privacy legislation and other applicable legislation
- Vulnerability and penetration testing has been completed
- Others……….

Cyber coverages can include…..

- Data breach and data compromise
- Restoration of data or recovery of data
- Extortion / Ransomware attack
- Business interruption and extra expense
- Misdirected payment fraud (for ex… Macewan University)
- Network security Liability
- Data compromise Liability
- Electronic Media Liability
- Others…
- Coverage is not standarized

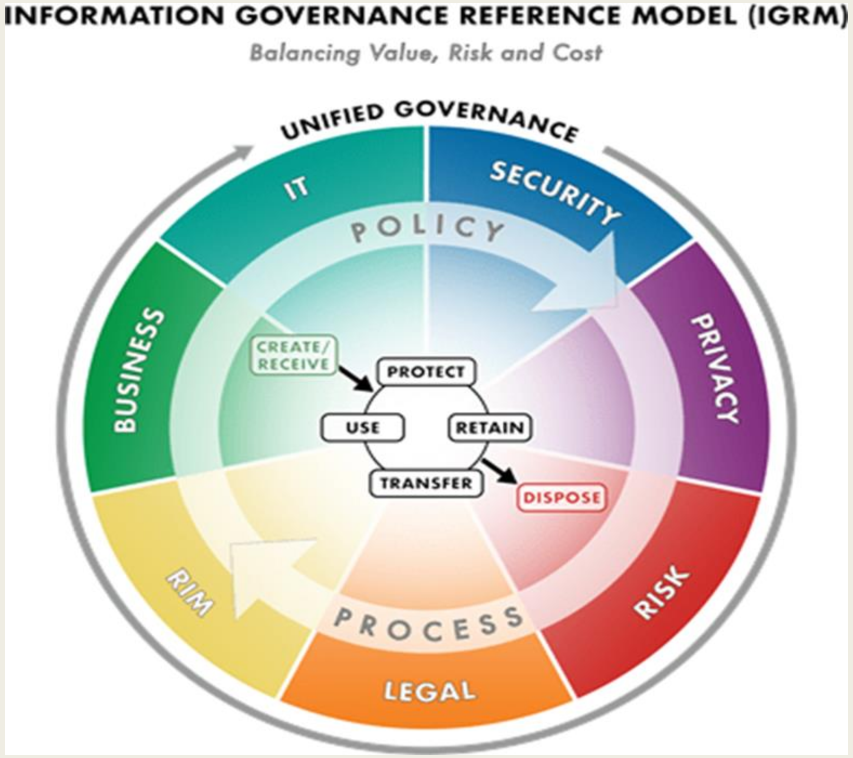
Cyber Insurance Coverage

Can provide

- Coverage for internet of things exposures
- Pre-breach offerings such as security education, security analysis, cyber security monitoring, penetration testing
- After a cyber event has been detected, professional services, including legal counsel, forensics, breach coaches, public relations and communications professionals, other specialized services to deal with the cyber event
- Because it’s not a matter of IF but WHEN

What’s your position on cyber?

Everyone has a role to play……
Cyber is everybody's business



Discussion and Questions