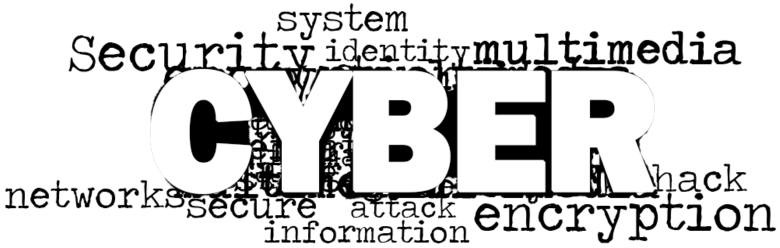


MRD
Training & Consulting Inc.

The Risks

Legal liability to others for computer/network security breaches

Legal liability to others for privacy breaches

Loss or damage to data / information

Loss of revenue due to a computer attack

Extra expense to recover / respond to a computer attack

Loss or damage to reputation

Regulatory actions and scrutiny

Cyber-extortion

Cyber-terrorism

Large Company Breaches

In 2016, 3 billion Yahoo accounts were hacked in one of the biggest breaches of all time. (Oath.com)

2016

In 2016, Uber reported that hackers stole the information of over 57 million riders and drivers. (Uber)

2016

In 2017, 412 million user accounts were stolen from Friendfinder’s sites. (LeakedSource)

2017

In 2017, 147.9 million consumers were affected by the Equifax Breach. (Equifax)

2017

In 2018, Under Armor reported that its “My Fitness Pal” was hacked, affecting 150 million users. (Under Armor)

2018

What about the little guys…..

61 percent of breach victims in 2017 were businesses with under 1,000 employees. (Verizon)

21 percent of all files are not protected in any way. (Varonis)

41 percent of companies have over 1,000 sensitive files including credit card numbers and health records left unprotected. (Varonis)

Nearly half of the security risk that organizations face stems from having multiple security vendors and products. (Cisco)

How often is this happening….

Thirty-one percent of organizations have experienced cyber attacks on operational technology infrastructure. (Cisco)

There are around 24,000 malicious mobile apps blocked every day. (Symantec)

Cryptojacking increased by 8,500 percent in 2017. (Symantec)

In 2017, 5.4 billion attacks by the WannaCry virus were blocked. (Symantec)

What’s the cost……

- The Equifax breach cost the company over $4 billion in total. (Time Magazine)

- The average cost per lost or stolen records per individual is $141 — but that cost varies per country. Breaches are most expensive in the United States ($225) and Canada ($190). (Ponemon Institute’s 2017 Cost of Data Breach Study)

- In companies with over 50k compromised records, the average cost of a data breach is $6.3 million. (Ponemon Institute’s 2017 Cost of Data Breach Study)

- Including turnover of customers, increased customer acquisition activities, reputation losses and diminished goodwill the cost of lost business globally was highest for U.S. companies at $4.13 million per company. (Ponemon Institute’s 2017 Cost of Data Breach Study)

In 2017, cyber crime costs accelerated with organizations spending nearly 23 percent more than 2016 — on average about $11.7 million. (Accenture)

The average cost of a malware attack on a company is $2.4 million. (Accenture)

The average cost in time of a malware attack is 50 days. (Accenture)

From 2016 to 2017 there was an 22.7 percentage increase in cybersecurity costs. (Accenture)

The average global cost of cyber crime increased by over 27 percent in 2017. (Accenture)

The most expensive component of a cyber attack is information loss, which represents 43 percent of costs. (Accenture)

Ransomware damage costs exceed $5 billion in 2017, 15 times the cost in 2015. (CSO Online)

What does the future look like….

- Damage related to cybercrime is projected to hit $6 trillion annually by 2021. (Cybersecurity Ventures)
- Ransomware attacks are growing more than 350 percent annually. (Cisco)
- IoT attacks were up 600 percent in 2017. (Symantec)
- The industry with the highest number of attacks by ransomware is the healthcare industry. Attacks will quadruple by 2020. (CSO Online)
- Ransomware damage costs will rise to $11.5 billion in 2019 and a business will fall victim to a ransomware attack every 14 seconds at that time. (Cybersecurity Ventures)
- Variants of mobile malware increased by 54 percent in 2017. (Symantec)

The Cyber Market

WOW!!!!!

DID I PEAK YOUR INTEREST YET???

CYBER
TERMS
RANSOMWARE
CYBERSECURITY
ATTACK
SMISHING
BRICKING
COMPUTER
ENGINEERING
VISHING
SOCIAL
BCDR
DDOS
SPYWARE
ADWARE
FIREWALL
UTM
BOTNET
MALWARE
WORM
TROJAN
LAYERED
ZERODAY
SPOOFING
PHISHING
VULNERABILITY

CLOUD COMPUTING

Top 10 Cloud Providers

aws

Azure

Google Cloud

Alibaba Cloud

salesforce

DELL

IBM

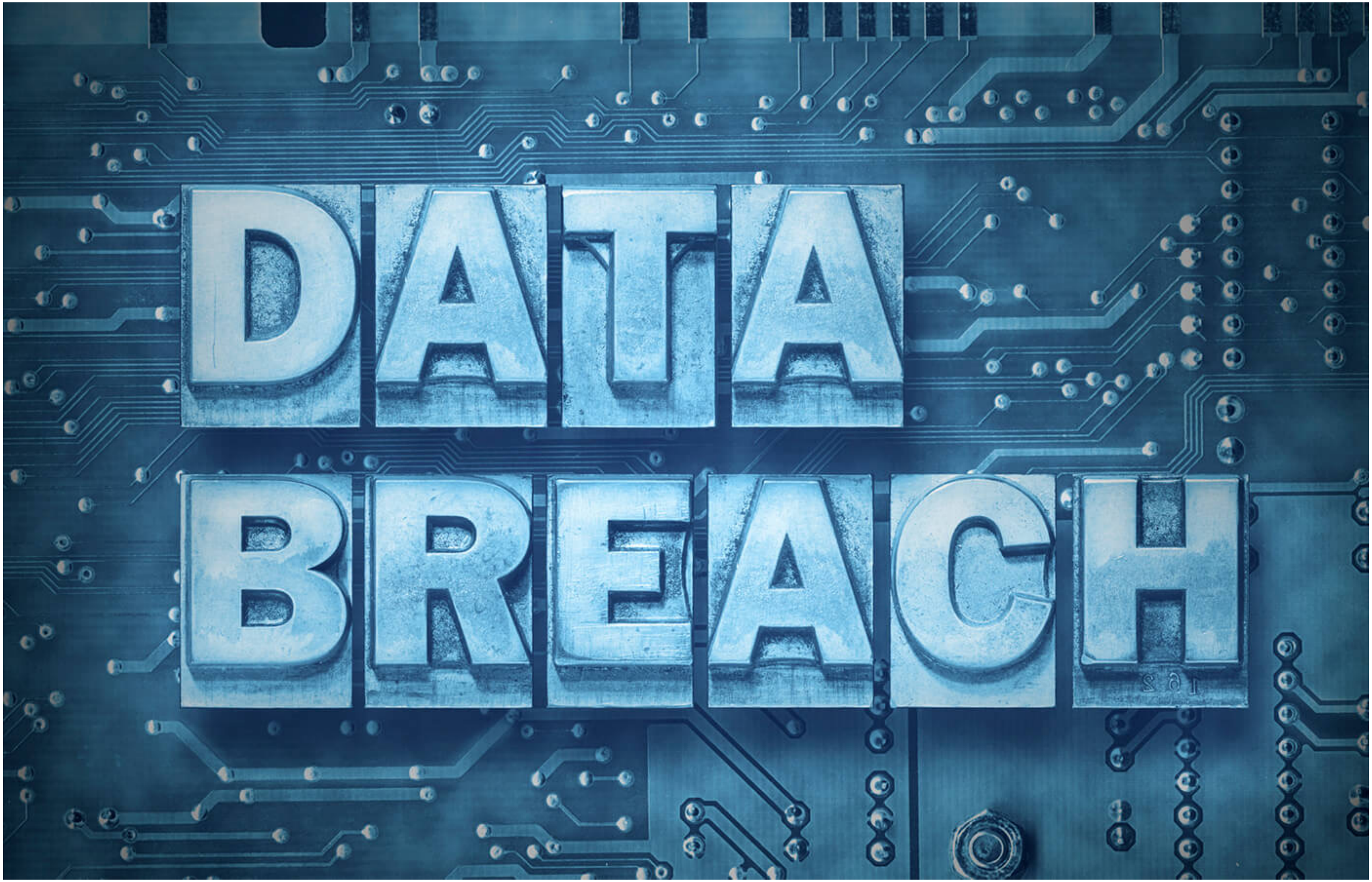
Digital Ocean

Dropbox

CYBER PERILS

CORPORATE BOGGING

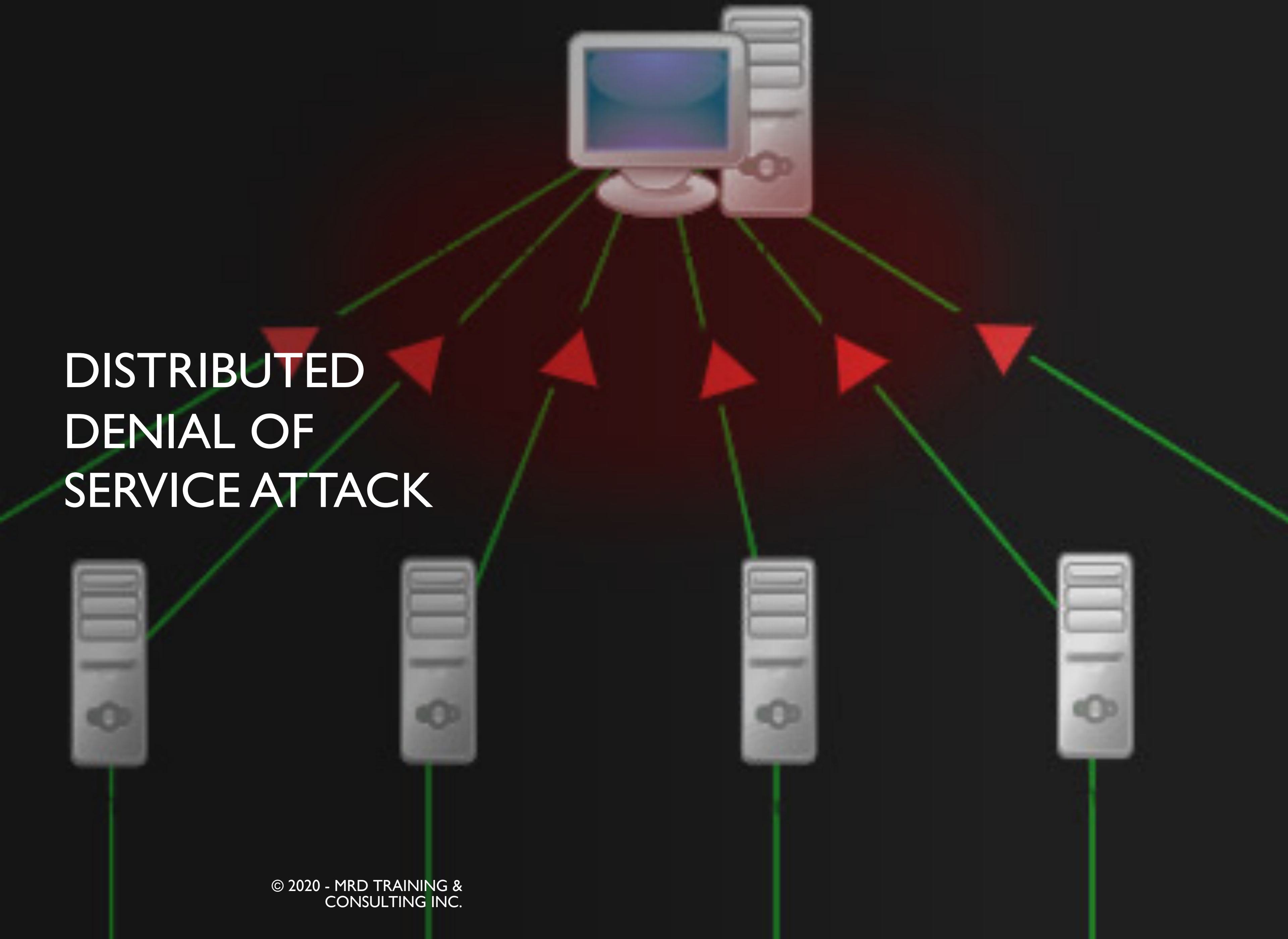
Creating or editing a web log, discussion forum post, online comment, or other associated social media activity where the primary purpose of that activity is to promote the insured or the individual’s position within insureds industry even if the nature of the content is not directly associated with insureds business activities


DATA
BREACH

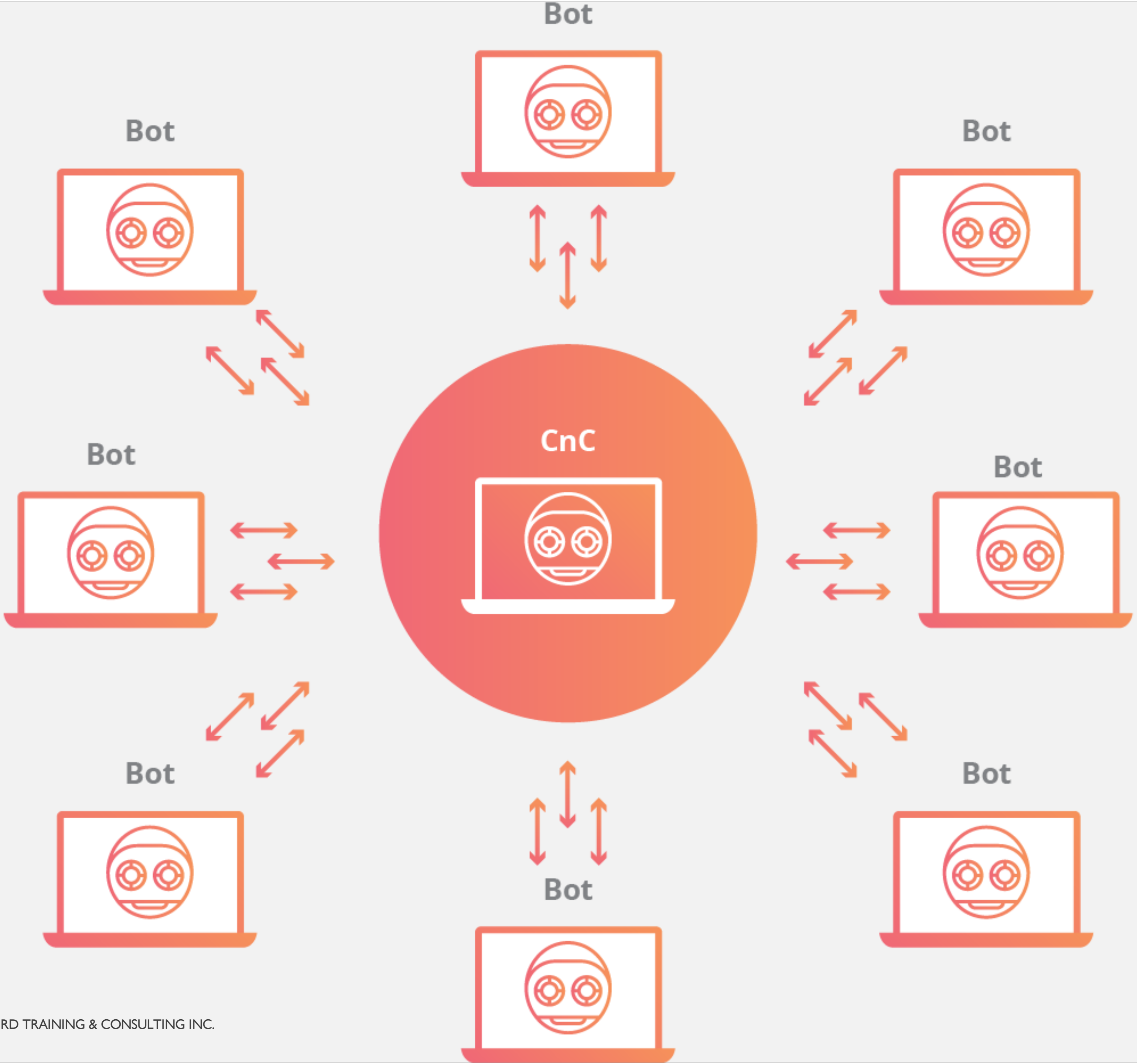
HACKING ATTACK

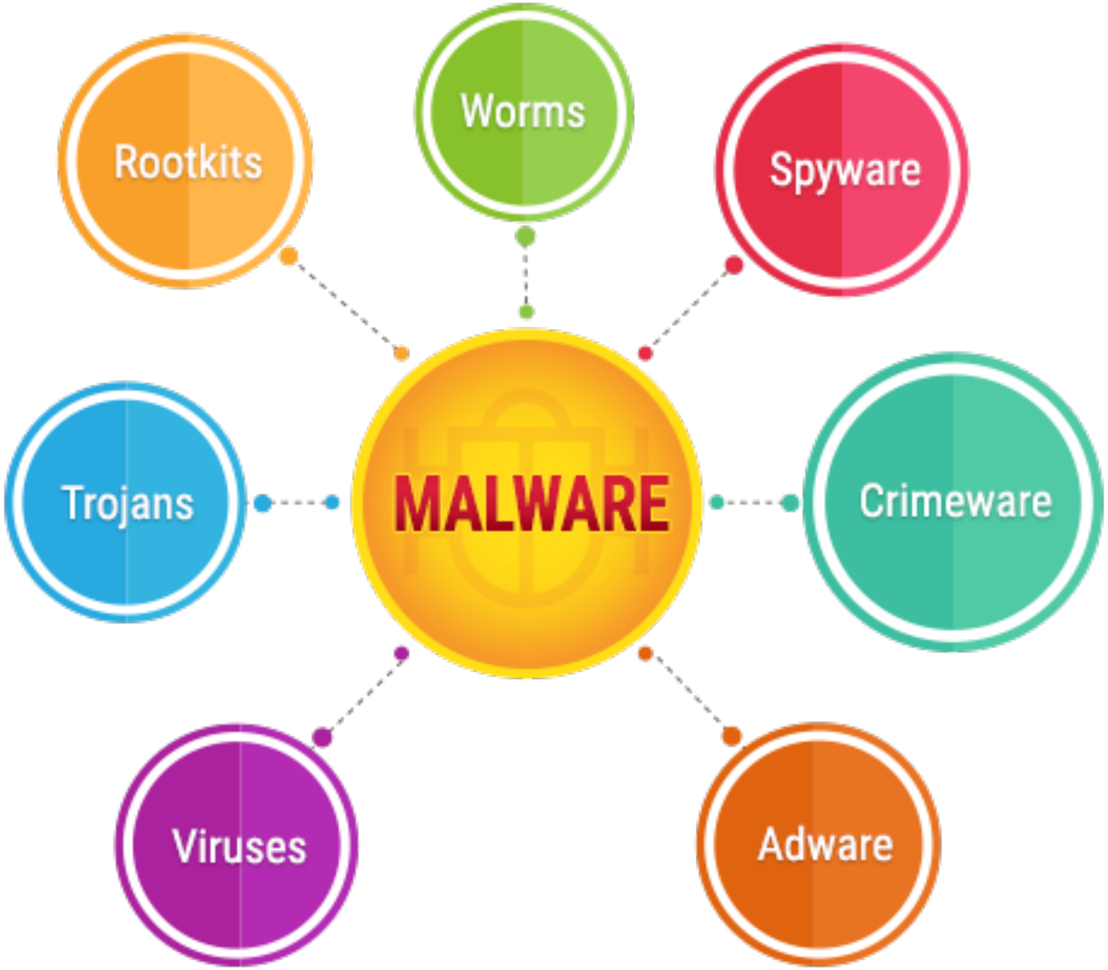
Any malicious or unauthorized electronic attack including but not limited to any fraudulent electronic signature, brute force attack, phishing, denial of service attack, that has been initiated by any third party or by any employee and that is designed to damage, destroy, corrupt, overload, circumvent or impair the functionality of computer systems.

DENIAL-OF-SERVICE
DoS ATTACK
DENIAL-OF-SERVICE
DoS ATTACK
DENIAL-OF-SERVICE
DoS ATTACK
DENIAL-OF-SERVICE
DoS ATTACK



DISTRIBUTED DENIAL OF SERVICE ATTACK


Bot
Bot
Bot
CnC
Bot
Bot
Bot
Bot
Bot


Rootkits
Worms
Spyware
Trojans
MALWARE
Crimeware
Viruses
Adware

SYSTEM OUTAGE PERIOD

Means the period during which the insured's computer systems or a cloud computing provider's systems are unavailable or operating at less than full operational capacity as a direct result of the cyber peril.

In the event of an intermittent problem causing repeated unavailability of systems as a direct result of the same proximate cause this will be deemed to be one continuous period.

The maximum system outage period is as stated in the Declarations and varies between companies.

USER
GENERATED
CONTENT

WE KEPT
CALM
AND WE
FINISHED STRONG
KeepCalmAndPosters.com

CYBER
INSURANCE

Let’s Talk First Party First….

Crisis Event Management Expenses

- Coverage for public relations services to mitigate negative publicity as a result of cyber liability

Security Breach Remediation and Notification Expenses

- Costs incurred to determine whose identity information was accessed
- Notification to those individuals of the security breach
- Credit monitoring
- Identity fraud expense reimbursement for those individuals affected by the security breach

Computer Program And Electronic Data Restoration

- Coverage for expenses incurred to restore data lost from damage to computer systems due to computer virus or unauthorized access

Computer Fraud & Funds Transfer Fraud

- Coverage for loss of money, securities or other property due to unauthorized access to computer system
- Coverage for loss of money or securities due to fraudulent transfer instructions to a financial institution

Reputation Guard

- Provides costs to restore Insured's reputation

Cyber Extortion

- Coverage for money paid due to threats made regarding an intent to fraudulently transfer funds, destroy data, introduce a virus or attack a computer system, or disclose electronic customer information
- Coverage for extortion demands by employees
- Network Extortion Demands - what is the currency language in the wording - will policy pay for demands for bitcoin, or only for government issued/regulated currency?

Cyber Media

- Coverage provided for numerous perils including copyright infringement, trademark infringement, defamation and invasion of privacy

Business Interruption

- Coverage for loss of income, and the extra expense incurred to restore operations, as a result of computer system disruption to the company's computer system caused by a virus or other unauthorized computer attack
- Coverage for loss of income, and the extra expense incurred to restore operations, as a result of a disruption to a service provider's computer system that the company relies on caused by a virus or other unauthorized computer attack

Social Engineering

- The use of deceptive tactics to manipulate people into volunteering sensitive information that is then leveraged for fraudulent purposes. Often, perpetrators use social engineering to harvest credentials for Account Takeover (ATO) or Corporate Account Takeover (CATO).

Let’s Talk Third Party Next….

Network and Information Security Liability

- Network and Information Security Liability
- Transmission of computer viruses
- Communications and Media Liability
- Regulatory and Defence Expenses

Let’s Talk About Exclusions

Raised
Practice
Collective
Standard
Competitive
Patent
Consider
Discovery
Global
Around
Power
Learn
Regulatory
Counsel
Reviews
Transactions
Market
Recent
Explore
Across
Investigations
Legal
Merger
Jurisdictions
Programs
Claim
Advertising
Increasingly
International
Government
Markets
Laws
FTC
Risks
Foreign
Pharmaceutical
Competition
Cooperation
Cartel
Enforcement
Approach
Protection
Fundamentals
Protect
Minority
Process
Damages
Consumer
Data
Program
Discuss
Challenges
Practitioners
Outside
Agencies
Parties
Analysis
Innovation
Economics
Best
Matters
Compliance
Antitrust
New
Effects
Security
Cases
Law
Economic
Rules
Concerns
Common
U.S
Federal
Conduct
Media
Standards
Distribution
Two-Sided
Developments
Anticompetitive
Enforcers
Ethics
Guidance
Latest
Litigation
Debate
Private
Practical
Provide
Consumers
Industry
Claims
Affect
Agency
Industries
Mergers
Practices
State
Individual

Claims and circumstances known at inception arising out of any security breach, crime, hacking attack or virus of which a senior executive officer was aware, or ought reasonably to have been aware, prior to the Inception Date of the Policy, whether notified under any other insurance or not.

RICO - for any actual or alleged violations of the Racketeer Influenced and Corrupt Organisation Act 18 USC Sections 1961 et seq and any amendments thereto, or any rules and regulations promulgated thereunder.

SEC - for any actual or alleged violation of any of the provisions of the Securities Act of 1933, the Securities Exchange Act 1934 or any similar regional, provincial, territorial, federal or state law or any common law relating thereto.

UNLAWFUL SURVEILLANCE

UNDERWRITING THE RISK

CHALLENGES TO UNDERWRITING CYBER

THE EVOLVING NATURE OF CYBER RISK

LIMITED CYBER LOSS EXPERIENCE

DIFFICULTIES IN ASSESSING POLICYHOLDER VULNERABILITIES

ACCUMULATION RISK

NON-AFFIRMATIVE EXPOSURE

Let’s Talk About The Legal Stuff

PIPEDA/PHIPA

- PIPEDA applies to Canadian companies.
- Governs collection, use, and disclosure of personal information.
- PHIPA deals with freedom of information and the protection of certain private (medical) information.
- Neither PIPEDA nor PHIPA provide a civil remedy for privacy infringement.

Bill S-4: Digital Privacy Act

Amendment to PIPEDA.

Requires organizations to inform consumers when their personal information has been lost or stolen.

Companies that fail to inform consumers or that destroy these records of a data breach will face fines up to $100,000.

Commissioner could publicly name organizations that are non-compliant if in the public interest.

U.S. Patriot Act

Allows U.S. law enforcement officials to seek a court order that allows access to the personal records of any person without that person's knowledge.

Officials could access information about citizens of other countries, including Canada, if that information is physically within the United States or accessible electronically.

Canadian companies that store information on American servers might have little control over that information.

Disclosure to U.S. officials might contravene PIPEDA or PHIPA.

THANK YOU!!!