CYBERSECURITY: Your Role and What You Need to Know

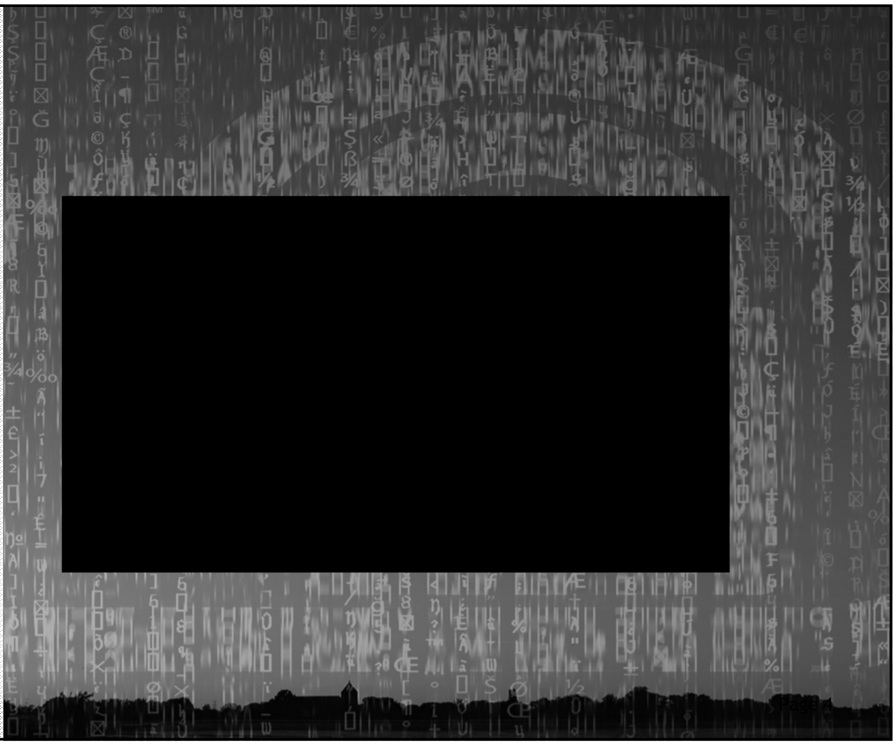
WITH YOU TODAY

Jamey Loupe
Senior Manager
IT Risk Advisory Services
+1 832-314-4104
jloupe@bdo.com

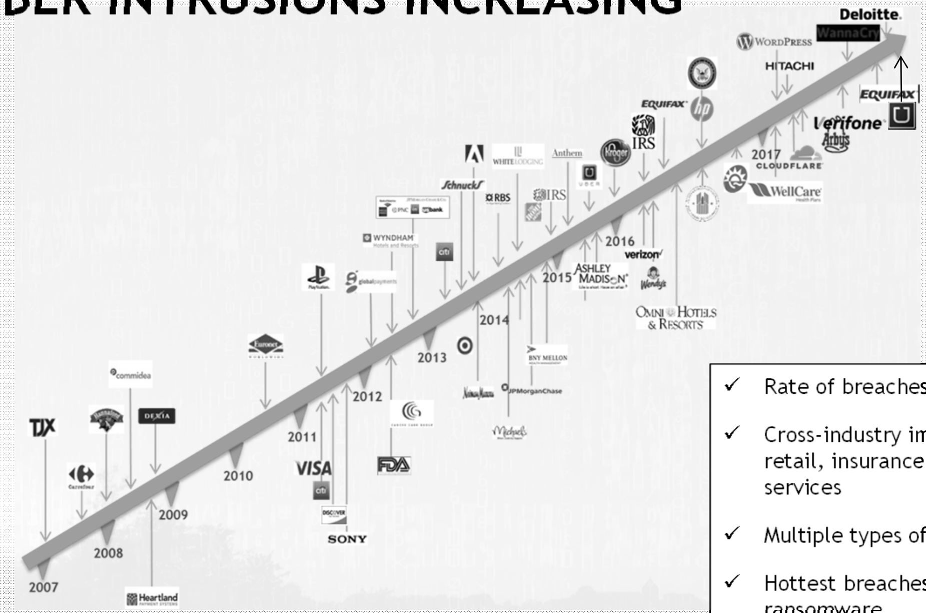
AGENDA

- Today's Threat Landscape and Types of Attacks
- Understanding Your Risk
- Cybersecurity Mitigation
- Conclusion

TODAY'S THREAT LANDSCAPE



CYBER INTRUSIONS INCREASING



- ✓ Rate of breaches increasing since 2007
- ✓ Cross-industry impact: healthcare, retail, insurance, technology, financial services
- ✓ Multiple types of breaches/threats
- ✓ Hottest breaches – phishing and ransomware

TODAY'S THREAT LANDSCAPE

CYBERSECURITY TODAY

It adds up…

The FBI estimates that ransomware this year will generate

$1 billion for criminals.

Businesses stand to lose much more from hacks—

at least **$400 billion** globally.

The cyberdefense, cyberforensics and cyberinsurance industries are projected to be worth nearly **$200 billion** annually by the close of the decade.

Time Magazine, December 19, 2016 "Person of the Year" (Excerpt of #3)

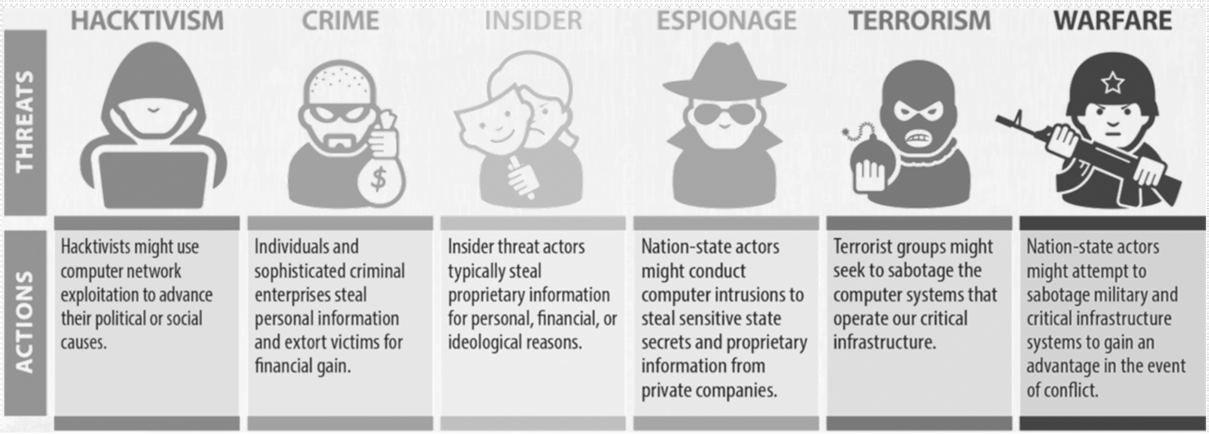
CYBERSECURITY TODAY

TODAY'S THREAT LANDSCAPE

Internal actors were responsible for **43%** of data loss, half of which is intentional, half accidental.

This year, companies that had data breaches involving less than 10,000 records, the average cost of data breach was $4.9 million and those companies with the loss or theft of more than 50,000 records had a cost of data breach of $13.1 million.

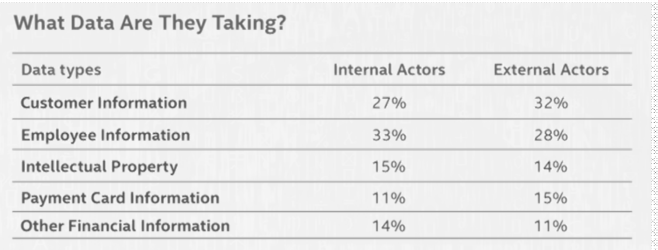
WHO ARE THE PLAYERS?



HACKTIVISM	CRIME	INSIDER	ESPIONAGE	TERRORISM	WARFARE
Hacktivists might use computer network exploitation to advance their political or social causes.	Individuals and sophisticated criminal enterprises steal personal information and extort victims for financial gain.	Insider threat actors typically steal proprietary information for personal, financial, or ideological reasons.	Nation-state actors might conduct computer intrusions to steal sensitive state secrets and proprietary information from private companies.	Terrorist groups might seek to sabotage the computer systems that operate our critical infrastructure.	Nation-state actors might attempt to sabotage military and critical infrastructure systems to gain an advantage in the event of conflict.

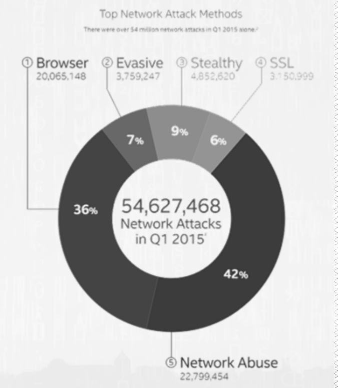
WHAT DO THEY WANT?

TODAY'S THREAT LANDSCAPE



What Data Are They Taking?

Data types	Internal Actors	External Actors
Customer Information	27%	32%
Employee Information	33%	28%
Intellectual Property	15%	14%
Payment Card Information	11%	15%
Other Financial Information	14%	11%



Top Network Attack Methods

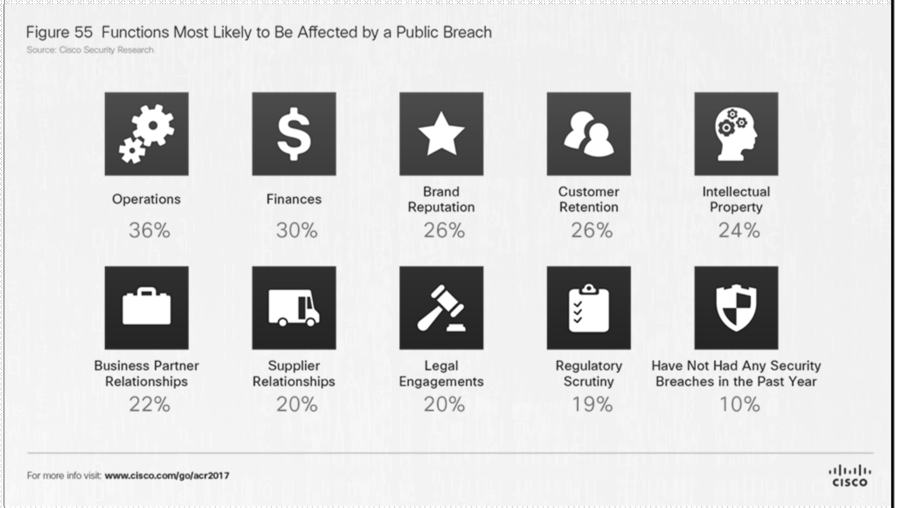
There were over 54 million network attacks in Q1 2015 alone.[2]

WHERE DO THEY ATTACK?

TODAY'S THREAT LANDSCAPE

Figure 55 Functions Most Likely to Be Affected by a Public Breach

Source: Cisco Security Research



For more info visit: **www.cisco.com/go/acr2017**

TODAY'S THREAT LANDSCAPE

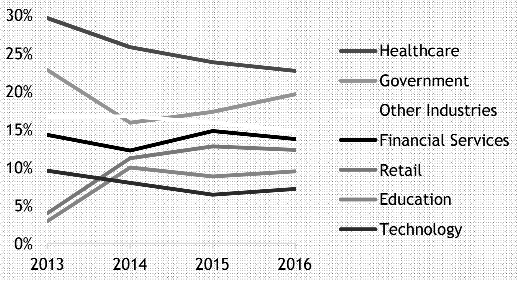
WHO DO THEY GO AFTER?

Healthcare and Financial Services are the most at-risk private-sector industries. However, every industry is becoming equally vulnerable over time

The largest targets of data breaches, Healthcare and Financial Services, are continuing to face increasing frequency of attacks. However, all other sectors such as Retail and Education are beginning to see many more attacks. Over time we are seeing an equalizing effect across industries.

Note: Government ranks highly because government organizations are the most likely to publically report breaches. Similarly, 'Other Industries' ranks highly, because it includes any industry not listed.

Data Breaches by Industry



Page 11

Source: Breach Level Index

TODAY'S THREAT LANDSCAPE

WHAT WILL IT COST YOU?

1.5 million
Cyber attacks each year
(approx. 4,000 per day)

16,856
Cyber attacks on
businesses each year

500 million
Yahoo user accounts
hacked

$2.1 trillion
Predicted global cost of data breaches by 2019

$74 billion ▶ **$1 trillion+**

Current annual spending on cybersecurity

Predicted global spending on cybersecurity 2017-2021

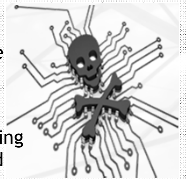
AGC New York, "Keeping Your Transactions Safe"

Page 12

MALWARE

COMMON TYPES OF ATTACKS

- A **computer virus** attaches itself to a program or file enabling it to spread from one computer to another, leaving infections as it travels.
- The **Trojan Horse**, at first glance will appear to be useful software but will actually do damage once installed or run on your computer.
- **Ransomware** holds your computer hostage by locking up your computer threatening to destroy data. Bad actors typically demand a payment for release of your data files.
- When a hacker connects a computer with other infected computers effectively creating an infected network, this is known as a **botnet**.
- **Spyware** secretly gathers private information about the user activity such as internet usage and logs keystrokes via the process of key locking to steal passwords and other sensitive data.



MALWARE

RANSOMWARE INCIDENTS

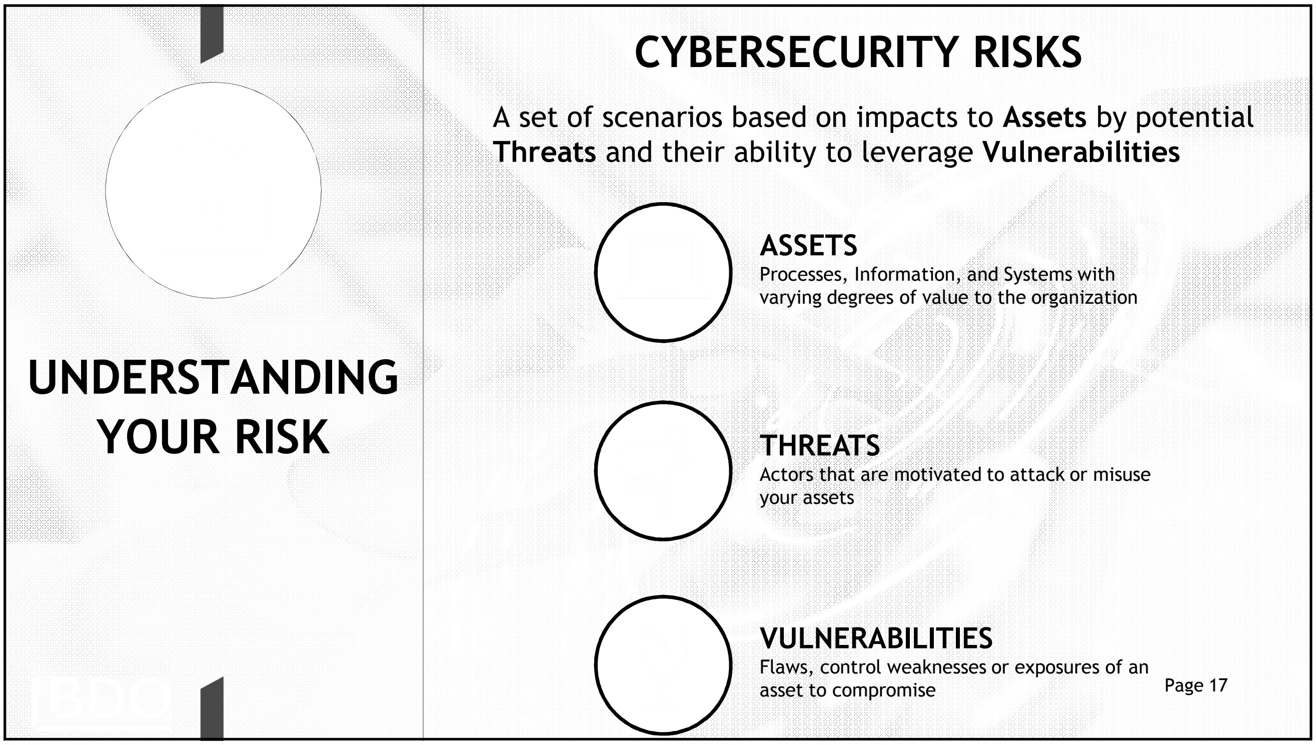
- March 2016, Hollywood Presbyterian Medical Center
  - Locked out of its EHR for a week
  - Providers were forced to revert to pen and paper
  - Decision was made to pay hackers $17,000 **in bitcoin**
- May 2018, Oil and Gas Construction Client
  - Ransomware attack
  - **Hackers encrypted all backup files, numerous servers, and over 40 employee computers.**
  - Locked out of email, entire network, and main ERP system for 9 days.
  - Estimated cost of $1.6M.
  - Hired numerous consultants to remediate issue and put preventive measures in place.
  - The FBI does not recommend that victims pay ransoms.

TODAY'S THREAT LANDSCAPE

WHY IS UNDERSTANDING LANDSCAPE IMPORTANT?

- The cyber security landscape is constantly evolving
- Since hackers only need to be right once and those who protect the organization need to be right all the time, your cyber security program needs to be constantly evolving also
- In order to evolve it is vital to understand who is after you, what motivates them and what they are after
- Understanding the landscape is a key element in any successful cyber security program

UNDERSTANDING YOUR RISK



UNDERSTANDING YOUR RISK

CYBERSECURITY RISKS

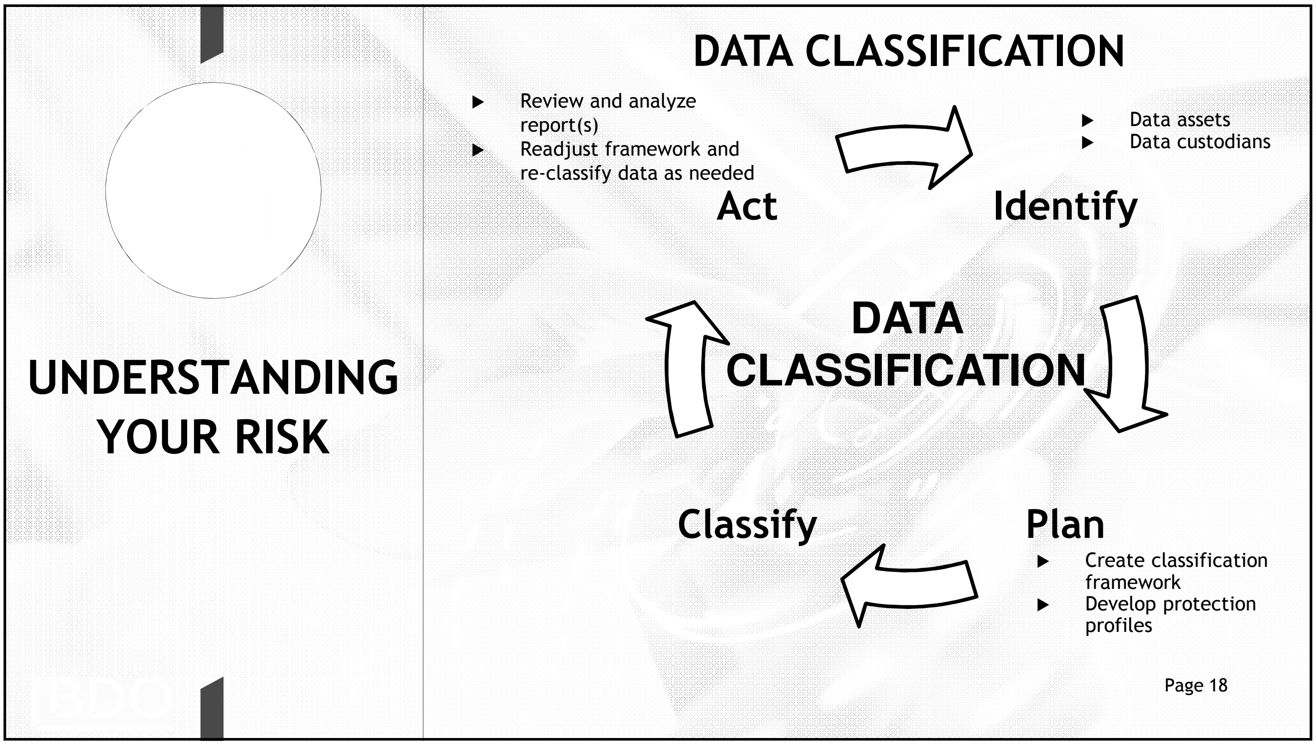
A set of scenarios based on impacts to **Assets** by potential **Threats** and their ability to leverage **Vulnerabilities**

ASSETS
Processes, Information, and Systems with varying degrees of value to the organization

THREATS
Actors that are motivated to attack or misuse your assets

VULNERABILITIES
Flaws, control weaknesses or exposures of an asset to compromise

Page 17



UNDERSTANDING YOUR RISK

DATA CLASSIFICATION

DATA CLASSIFICATION

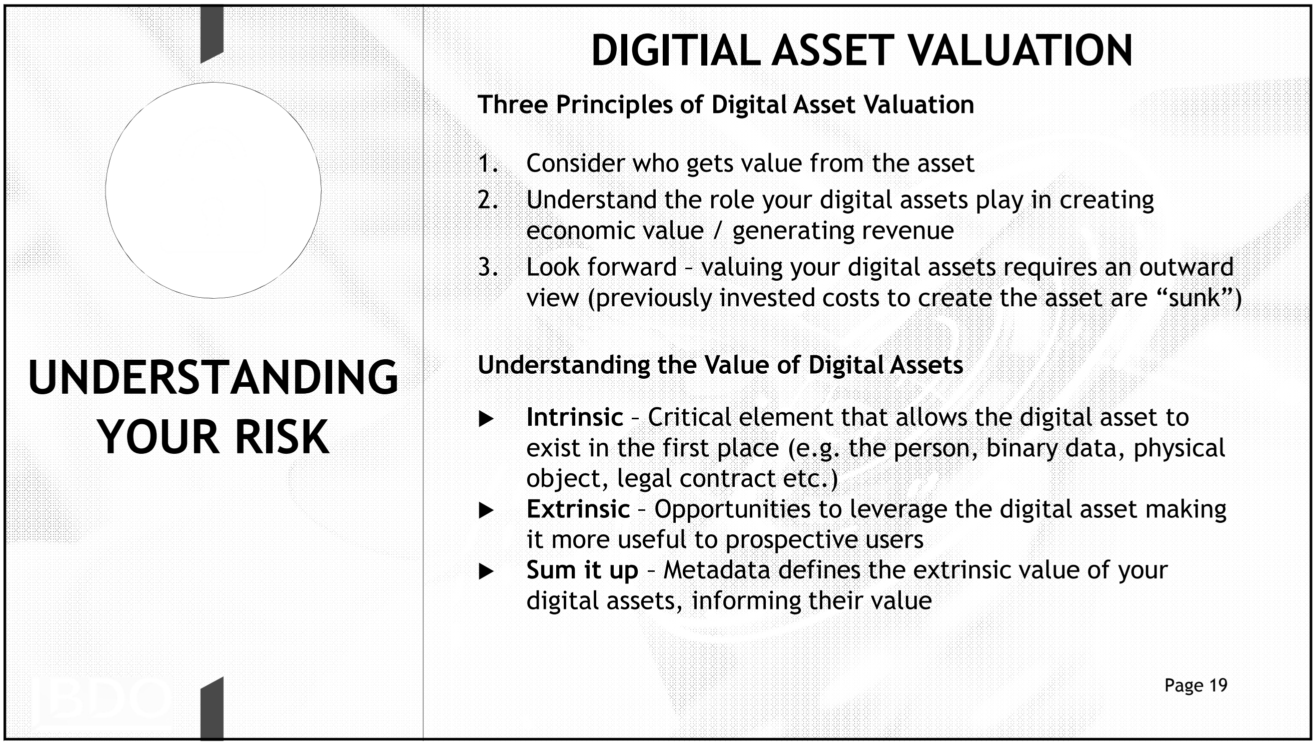
Identify
- Data assets
- Data custodians

Plan
- Create classification framework
- Develop protection profiles

Classify

Act
- Review and analyze report(s)
- Readjust framework and re-classify data as needed

Page 18



UNDERSTANDING YOUR RISK

DIGITIAL ASSET VALUATION

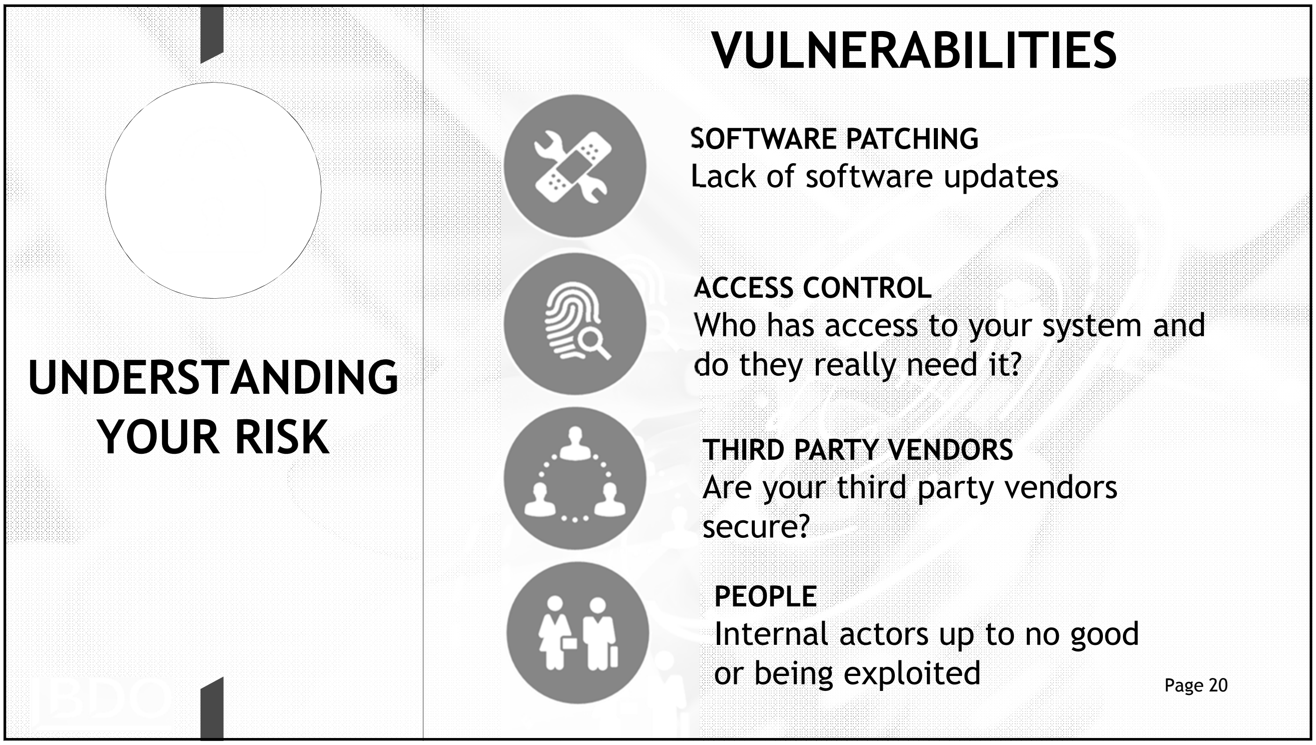
Three Principles of Digital Asset Valuation

1. Consider who gets value from the asset
2. Understand the role your digital assets play in creating economic value / generating revenue
3. Look forward – valuing your digital assets requires an outward view (previously invested costs to create the asset are “sunk”)

Understanding the Value of Digital Assets

- **Intrinsic** – Critical element that allows the digital asset to exist in the first place (e.g. the person, binary data, physical object, legal contract etc.)
- **Extrinsic** – Opportunities to leverage the digital asset making it more useful to prospective users
- **Sum it up** – Metadata defines the extrinsic value of your digital assets, informing their value

Page 19



UNDERSTANDING YOUR RISK

VULNERABILITIES

SOFTWARE PATCHING
Lack of software updates

ACCESS CONTROL
Who has access to your system and do they really need it?

THIRD PARTY VENDORS
Are your third party vendors secure?

PEOPLE
Internal actors up to no good or being exploited

Page 20

UNDERSTANDING YOUR RISK

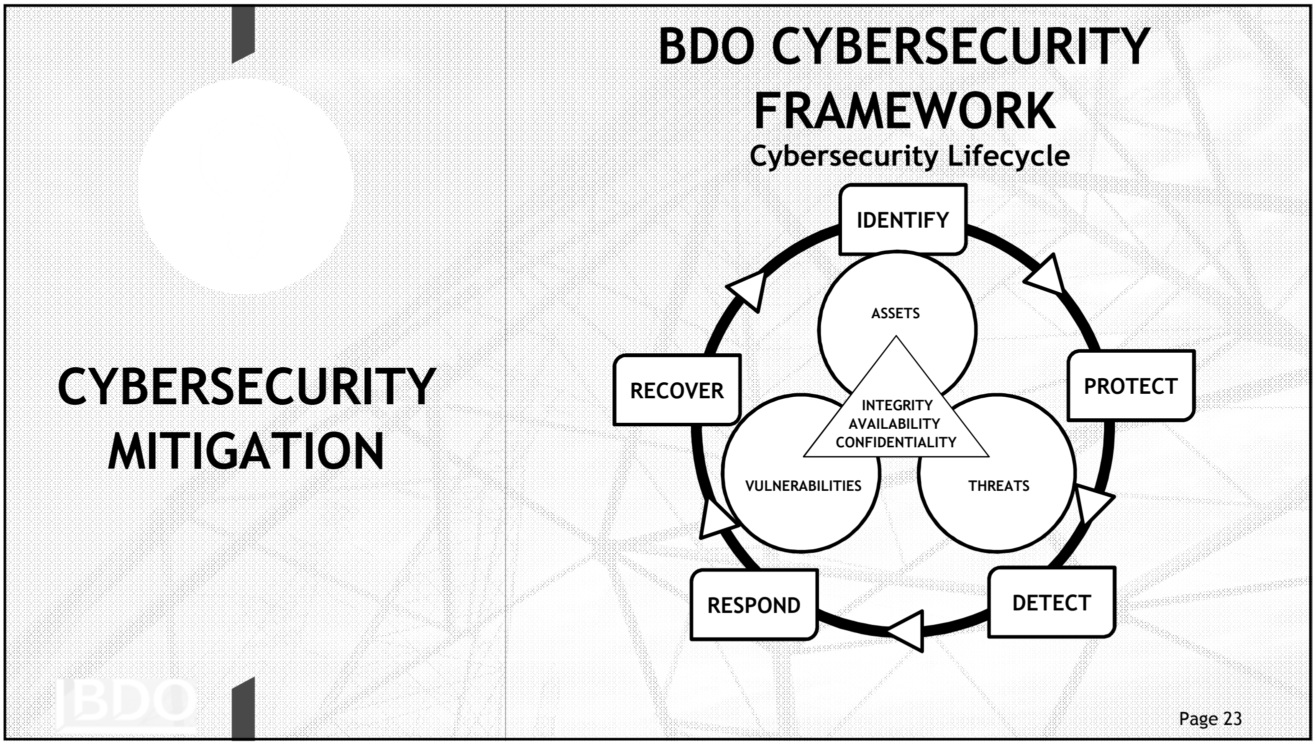
AND THE BIGGEST RISK IS – YOU!

THIRD PARTY VENDORS
Are your third party vendors secure?

PEOPLE
Internal actors up to no good or being exploited

Trusted users are the biggest single vulnerability. Most exploits enter the environment because of or through manipulation of trusted.

CYBERSECURITY MITIGATION

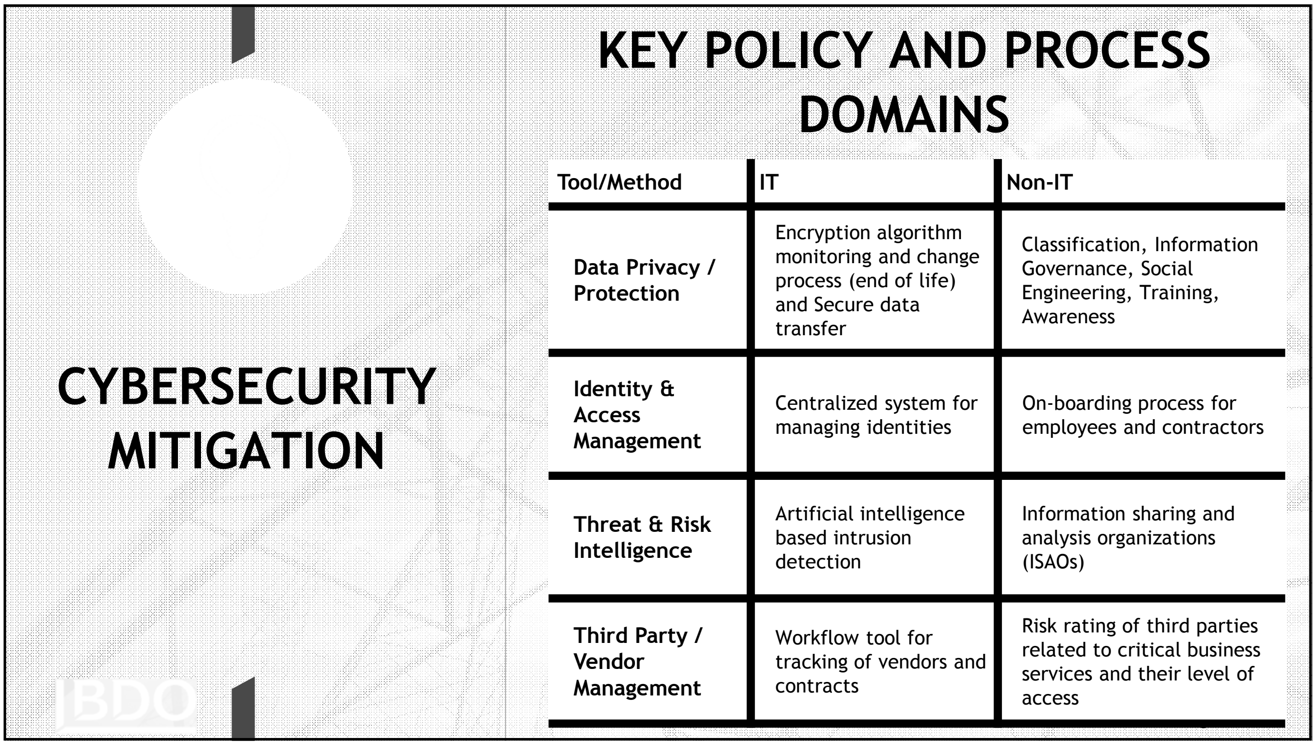


CYBERSECURITY MITIGATION

BDO CYBERSECURITY FRAMEWORK

Cybersecurity Lifecycle

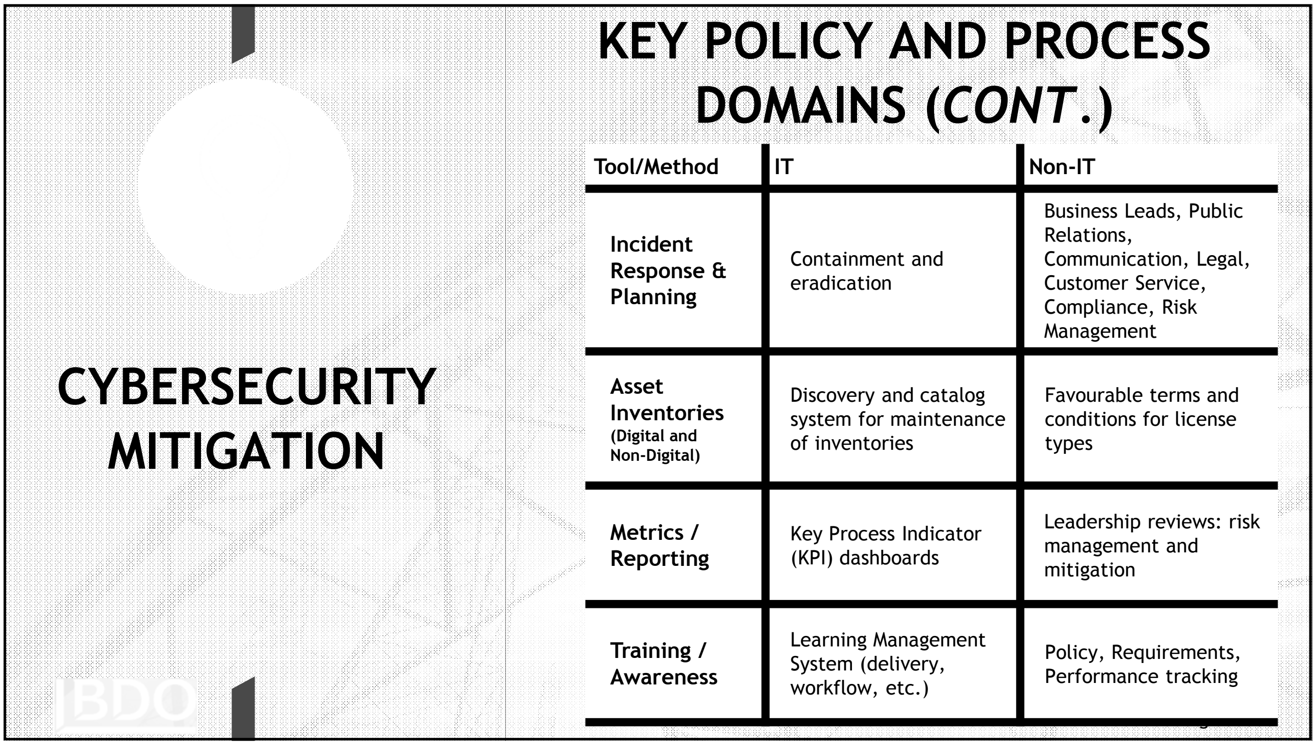
Page 23



CYBERSECURITY MITIGATION

KEY POLICY AND PROCESS DOMAINS

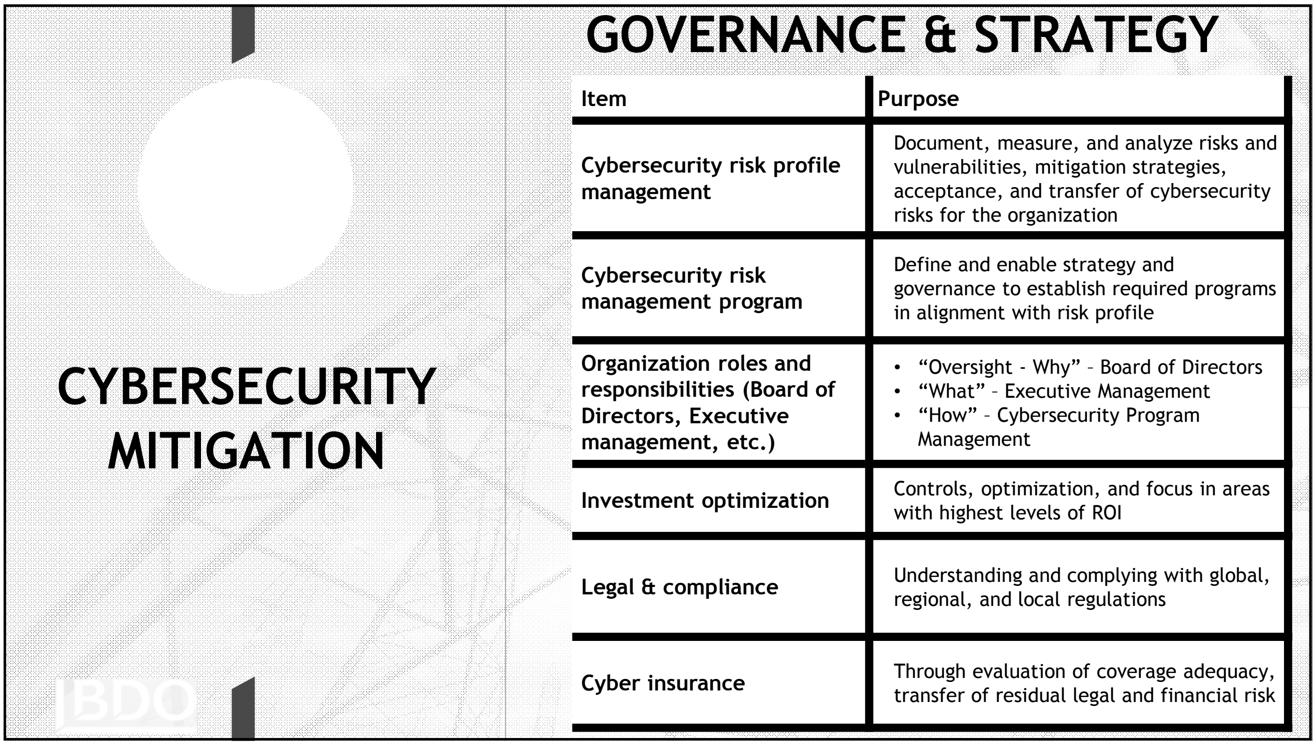
Tool/Method	IT	Non-IT
Data Privacy / Protection	Encryption algorithm monitoring and change process (end of life) and Secure data transfer	Classification, Information Governance, Social Engineering, Training, Awareness
Identity & Access Management	Centralized system for managing identities	On-boarding process for employees and contractors
Threat & Risk Intelligence	Artificial intelligence based intrusion detection	Information sharing and analysis organizations (ISAOs)
Third Party / Vendor Management	Workflow tool for tracking of vendors and contracts	Risk rating of third parties related to critical business services and their level of access



CYBERSECURITY MITIGATION

KEY POLICY AND PROCESS DOMAINS (*CONT*.)

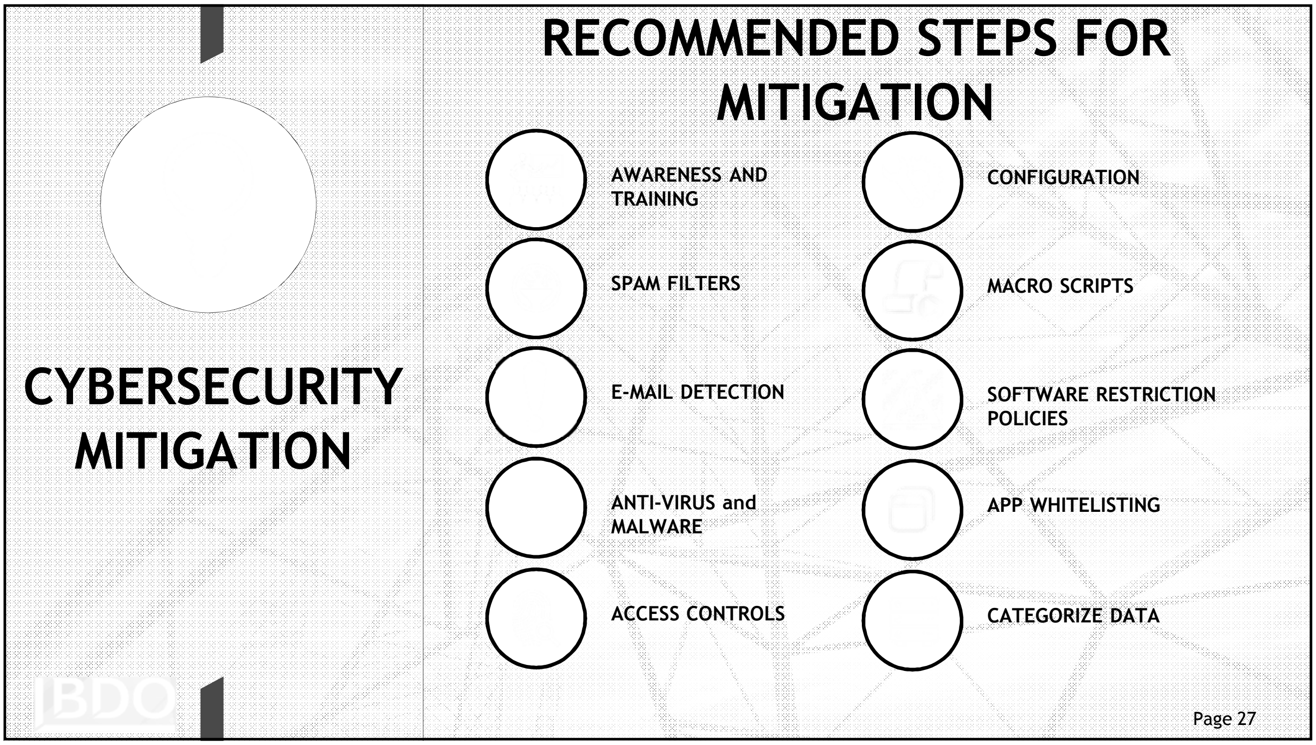
Tool/Method	IT	Non-IT
Incident Response & Planning	Containment and eradication	Business Leads, Public Relations, Communication, Legal, Customer Service, Compliance, Risk Management
Asset Inventories **(Digital and Non-Digital)**	Discovery and catalog system for maintenance of inventories	Favourable terms and conditions for license types
Metrics / Reporting	Key Process Indicator (KPI) dashboards	Leadership reviews: risk management and mitigation
Training / Awareness	Learning Management System (delivery, workflow, etc.)	Policy, Requirements, Performance tracking



CYBERSECURITY MITIGATION

GOVERNANCE & STRATEGY

Item	Purpose
Cybersecurity risk profile management	Document, measure, and analyze risks and vulnerabilities, mitigation strategies, acceptance, and transfer of cybersecurity risks for the organization
Cybersecurity risk management program	Define and enable strategy and governance to establish required programs in alignment with risk profile
Organization roles and responsibilities (Board of Directors, Executive management, etc.)	• “Oversight - Why” – Board of Directors • “What” – Executive Management • “How” – Cybersecurity Program Management
Investment optimization	Controls, optimization, and focus in areas with highest levels of ROI
Legal & compliance	Understanding and complying with global, regional, and local regulations
Cyber insurance	Through evaluation of coverage adequacy, transfer of residual legal and financial risk

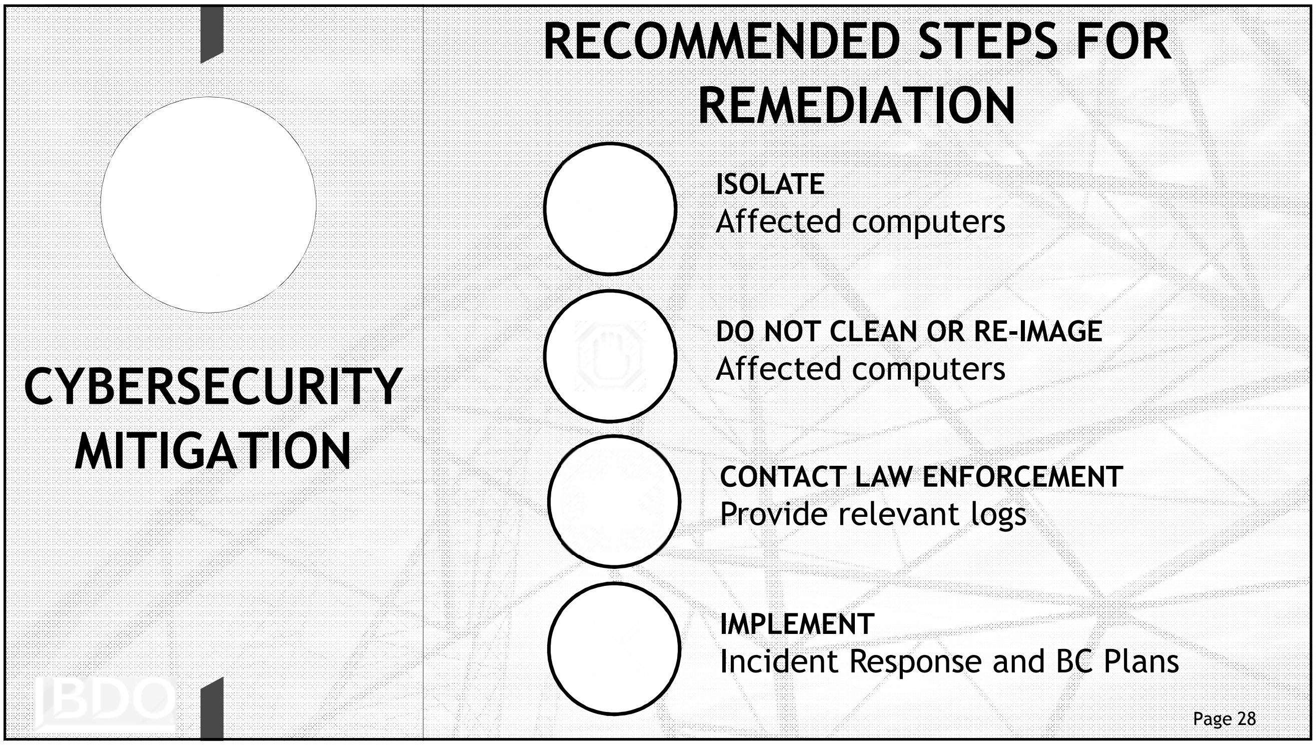


CYBERSECURITY MITIGATION

RECOMMENDED STEPS FOR MITIGATION

- AWARENESS AND TRAINING
- SPAM FILTERS
- E-MAIL DETECTION
- ANTI-VIRUS and MALWARE
- ACCESS CONTROLS
- CONFIGURATION
- MACRO SCRIPTS
- SOFTWARE RESTRICTION POLICIES
- APP WHITELISTING
- CATEGORIZE DATA

Page 27



CYBERSECURITY MITIGATION

RECOMMENDED STEPS FOR REMEDIATION

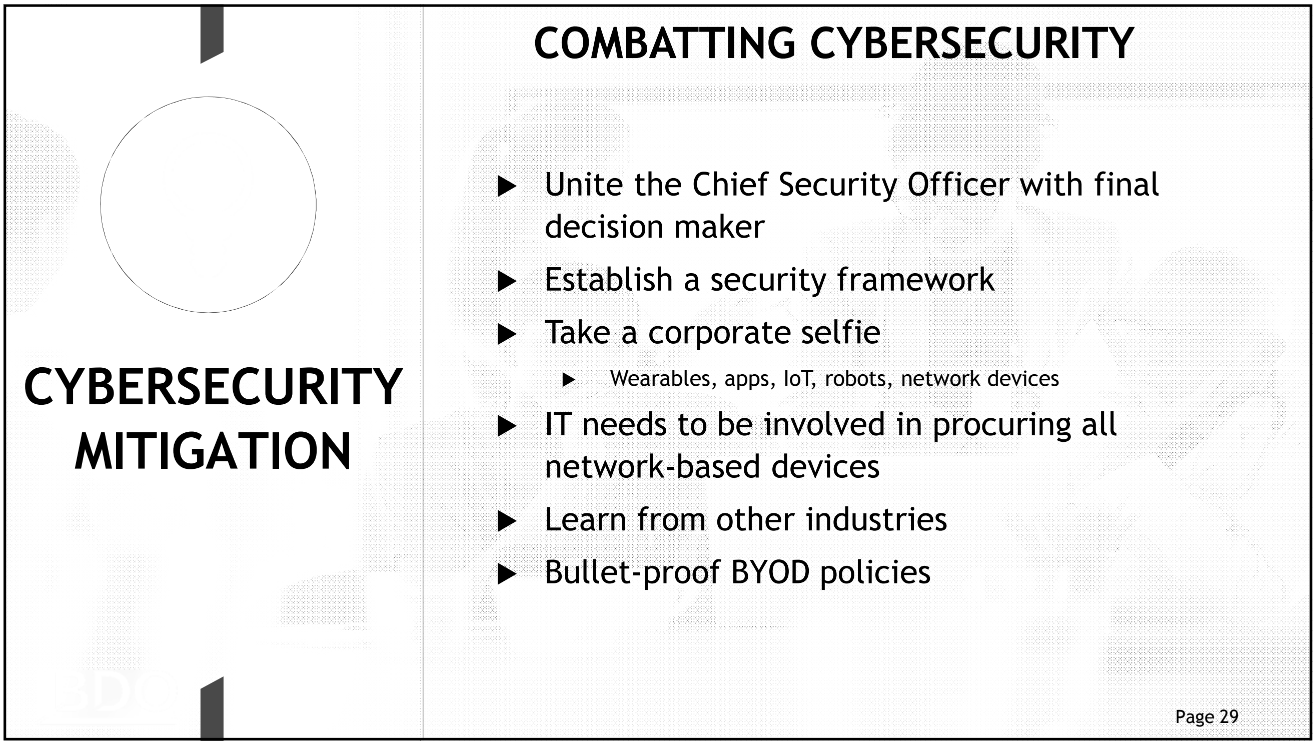
ISOLATE
Affected computers

DO NOT CLEAN OR RE-IMAGE
Affected computers

CONTACT LAW ENFORCEMENT
Provide relevant logs

IMPLEMENT
Incident Response and BC Plans

Page 28



CYBERSECURITY MITIGATION

COMBATTING CYBERSECURITY

- Unite the Chief Security Officer with final decision maker
- Establish a security framework
- Take a corporate selfie
  - Wearables, apps, IoT, robots, network devices
- IT needs to be involved in procuring all network-based devices
- Learn from other industries
- Bullet-proof BYOD policies

Page 29

CONCLUSION

Page 30

SPEAKER BIO

Jamey Loupe
Senior Manager
IT Risk Advisory Services
+1 832-314-4104
jloupe@bdo.com

Jamey is a Senior Manager within the Risk Advisory Services group at BDO USA, LLP. He has over 15 years of progressive experience leading and organizing teams and projects. He has provided audit and advisory services to various Fortune 500 and mid-size multi-national companies in multiple industries. Prior to joining BDO, Jamey worked in the Internal Audit and IT Security functions for Oil and Gas services companies. Prior to that he was with PricewaterhouseCoopers.

Throughout his career, Jamey has led and supported the activities needed to complete the audit process. He has experience presenting results to Senior Management and the Audit Committee. His experience includes:

- Leading, managing and conducting IT internal audits
- Managing complex IT SOX compliance projects
- Recommending and implementing IT process improvements
- Conducting and leading ERP pre and post implementation reviews
- Conducting IT security assessments

Jamey has further experience in Information Technology Standards & Governance, IT Risk Assessments, Cloud Security and Governance, and Disaster Recover Planning.

ABOUT BDO CONSULTING
BDO Consulting, a division of BDO USA, LLP, provides clients with Financial Advisory, Business Advisory and Technology Services in the U.S. and around the world, leveraging BDO's global network of more than 67,000 professionals. Having a depth of industry expertise, we provide rapid, strategic guidance in the most challenging of environments to achieve exceptional client service.

BDO is the brand name for BDO USA, LLP, a U.S. professional services firm providing assurance, tax, advisory and consulting services to a wide range of publicly traded and privately held companies. For more than 100 years, BDO has provided quality service through the active involvement of experienced and committed professionals. The firm serves clients through more than 60 offices and over 500 independent alliance firm locations nationwide. As an independent Member Firm of BDO International Limited, BDO serves multi-national clients through a global network of 1,400 offices across 158 countries.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. For more information please visit: www.bdo.com.

Material discussed is meant to provide general information and should not be acted on without professional advice tailored to your firm's individual needs.