Cybersecurity Risk Management

Threats, Challenges, and Frameworks

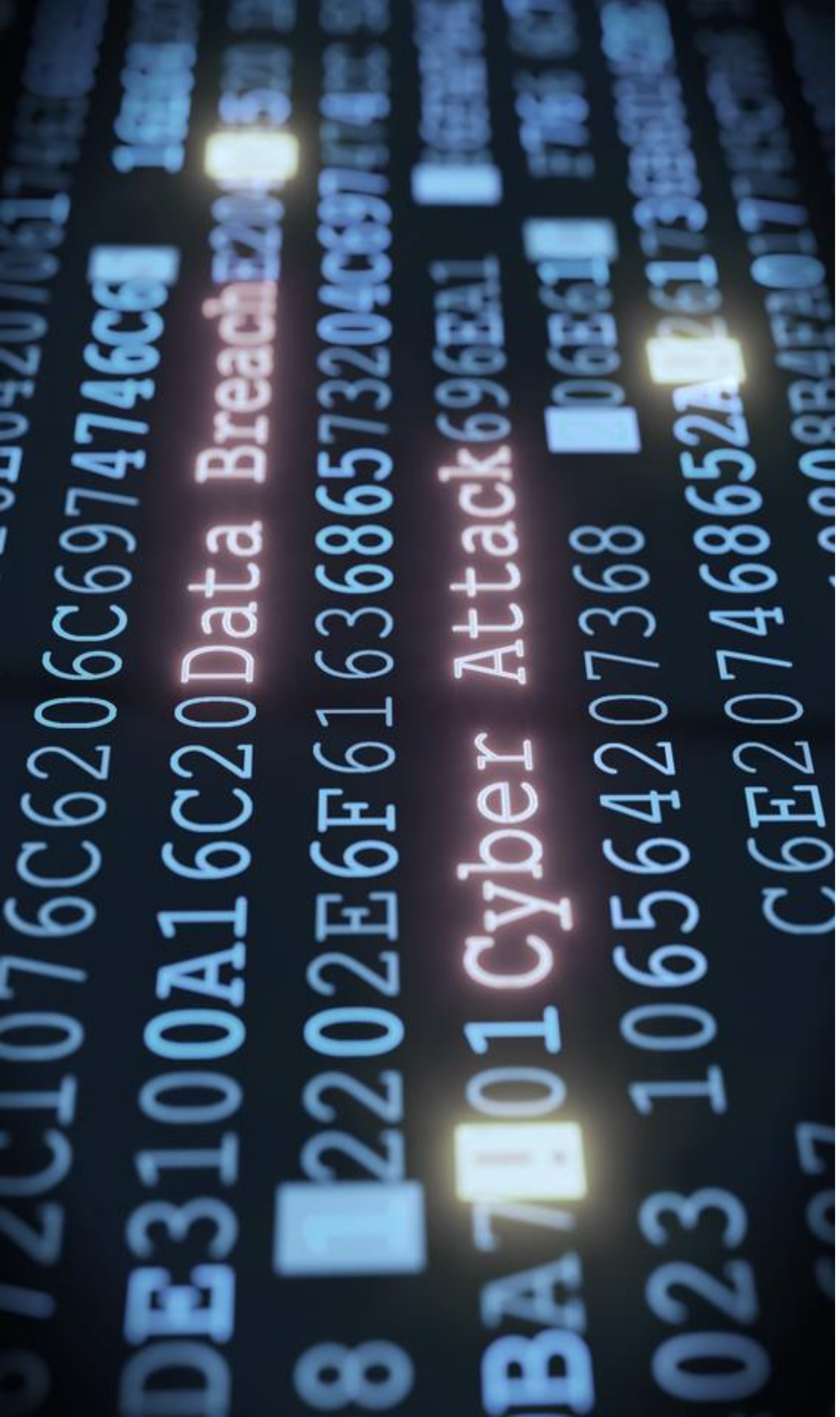
John Banghart
Senior Director   +1 202.344.4803 JFBanghart@Venable.com

VENABLE LLP

Who am I?

- 30 years in information technology and information security
  - 2 years with the White House National Security Council as Director for Federal Cybersecurity under President Barack Obama.
  - 4 years with the National Institute of Standards and Technology Cybersecurity Division.
  - 5 years with the Center for Internet Security
  - 1 year with Microsoft Azure.
  - Other years with Miscellaneous
- Over 6 years with Venable, helping clients and the global community tackle cybersecurity risk and policy issues.

VENABLE LLP



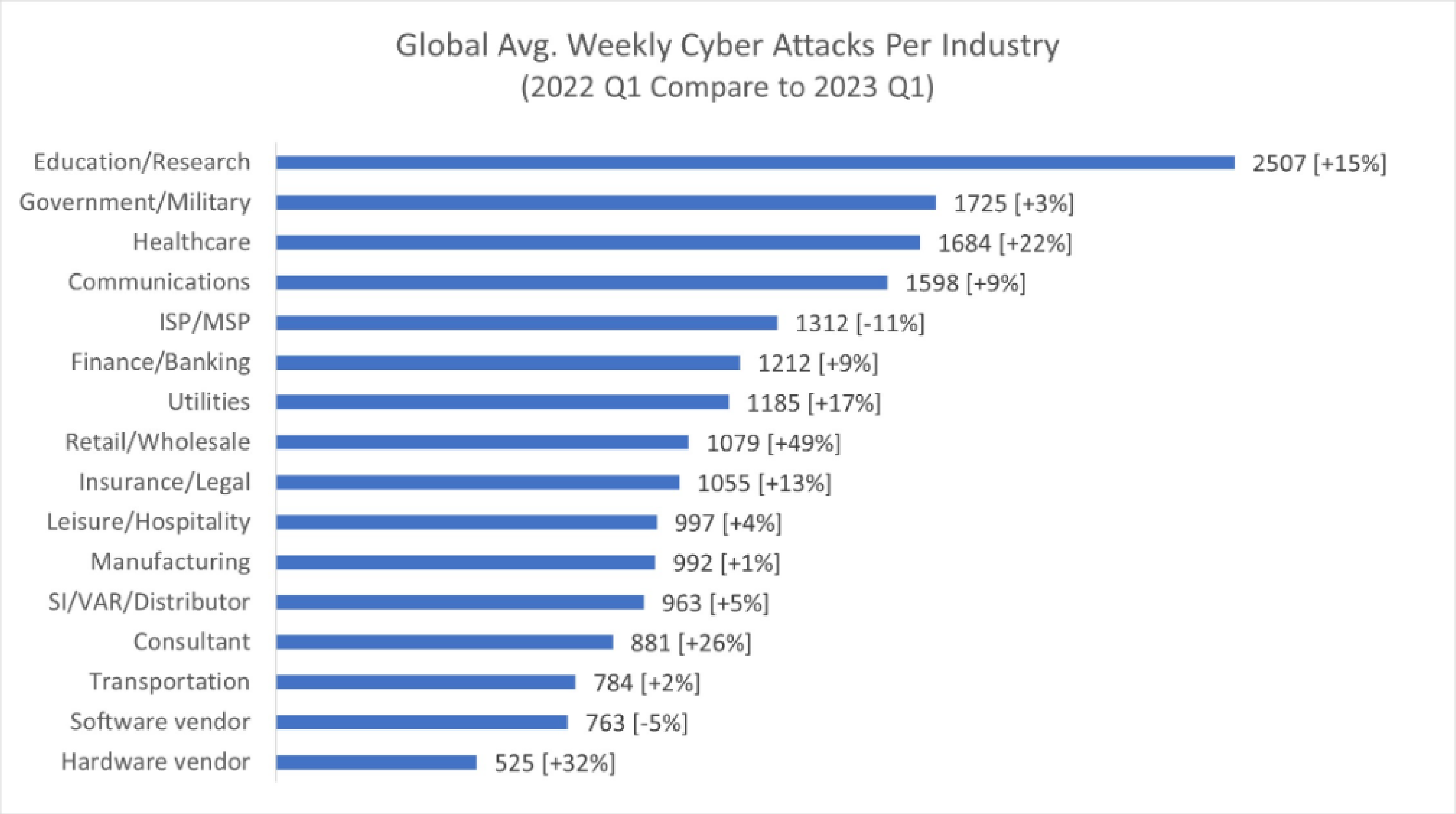
The Threat

Nation States

Organized Crime

Hacktivists

The Threat

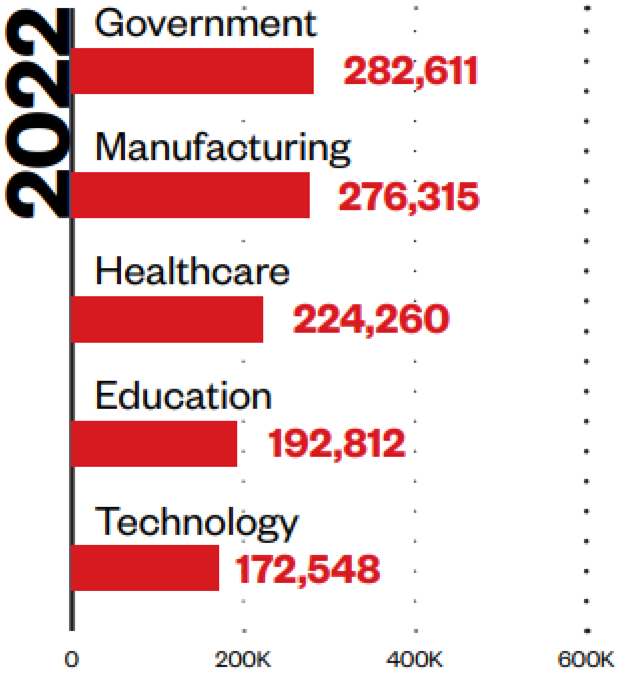


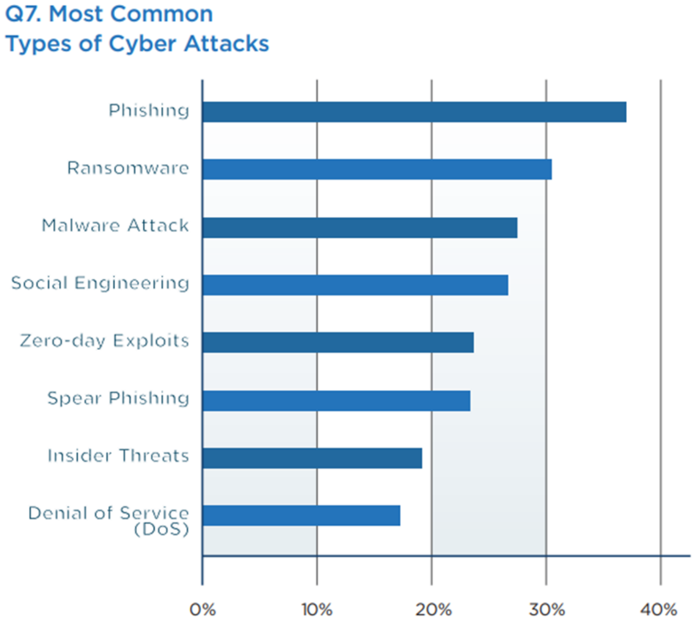
Global average cyberattacks per industry Image: Check Point Software Technologies

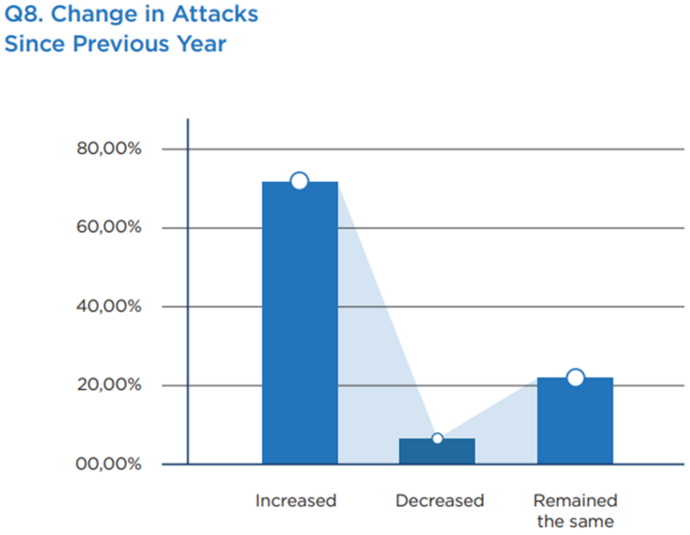
VENABLE LLP

The Threat

Malicious File Detections

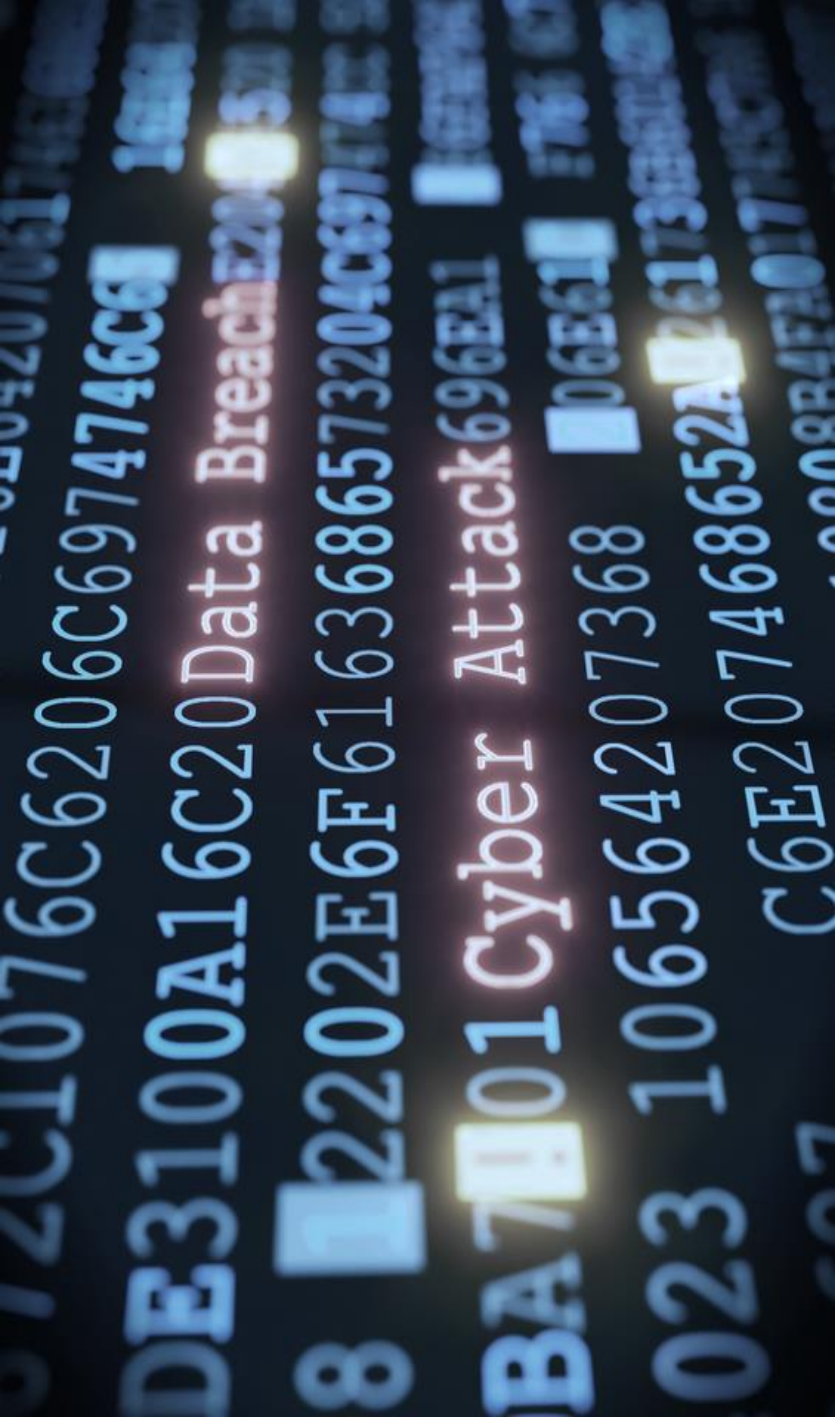






VENABLE LLP

Sources: Trend Micro *Annual Cybersecurity Round Up 2022*; LATAM CISO Report 2022



What You Can Do Better to Manage Cybersecurity Risk

People

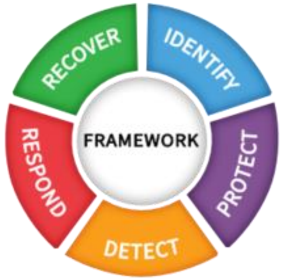
Process

Technology

First - Adopt Risk-based International Standards and Frameworks

□ **NIST Cybersecurity Framework (CSF)**

- Voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk
- Adaptable regardless of organization size, budget, maturity
- NIST CSF Profile - Ransomware



□ **ISO/IEC 27000 Series**

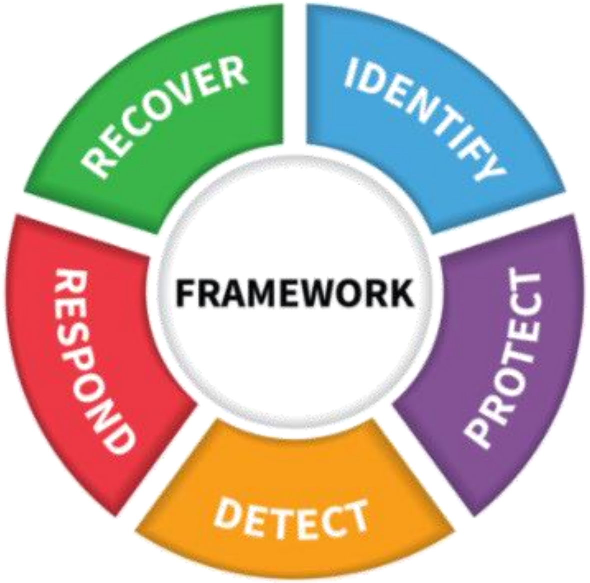
  - International information security standards

VENABLE LLP

Sources: National Institute of Standards and Technology (NIST)

NIST Cybersecurity Framework

- Risk-based cybersecurity outcomes
- Review priorities and gaps; align legal/regulatory requirements and organizational and risk management priorities
- Common and accessible terminology
- Connected to and based on international standards
- Adaptable to many technologies, lifecycle phases, sectors and uses
- Guided by many perspectives – private sector, academia, public sector



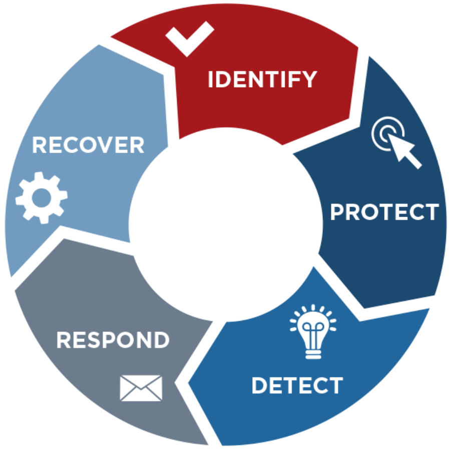
1 IDENTIFY

Identify and control who has access to your business information

Conduct background checks

Require individual user accounts for each employee

Create policies and procedures for cybersecurity



2 PROTECT

Limit employee access to data and information

Install Surge Protectors and Uninterruptible Power Supplies (UPS)

Patch your operating systems and applications routinely

Install and activate software and hardware firewalls on all your business networks

Secure your wireless access point and networks

Set up web and email filters

Use encryption for sensitive business information

Dispose of old computers and media safely

Train your employees

3 DETECT

Install and update anti-virus, anti-spyware, and other anti-malware programs

Maintain and monitor logs

4 RESPOND

Develop a plan for disasters and information security incidents

5 RECOVER

Make full backups of important business data and information

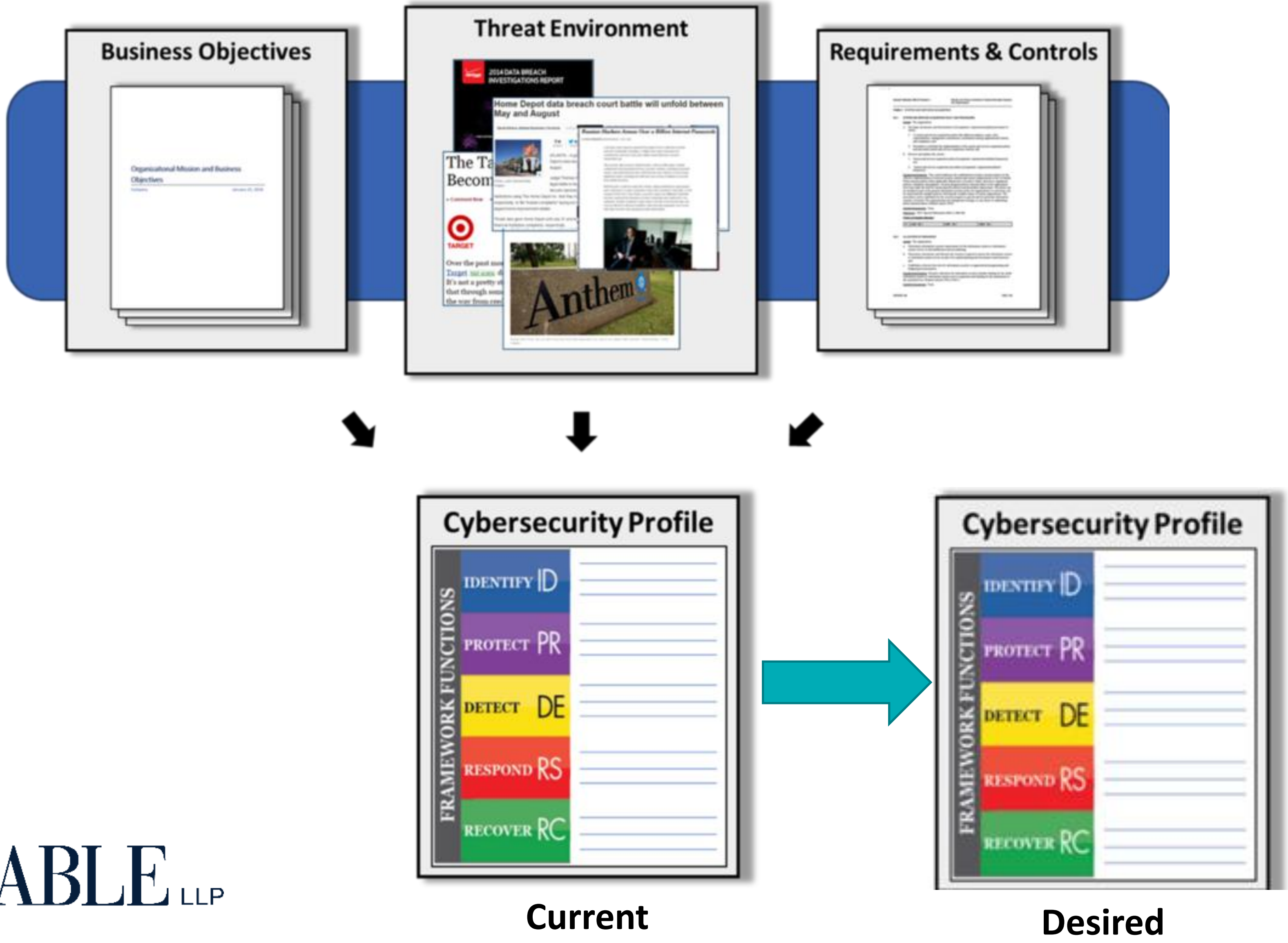
Continue to schedule incremental backups

Consider cyber insurance

Make improvements to processes/ procedures/ technologies

VENABLE LLP

NIST Framework Profile



VENABLE LLP

5 Other Actions to Increase Preparedness and Reduce Liability

- **Conduct Assessments Tied to the NIST Cybersecurity Framework**
  - Risk Management Focus
  - Requirements and review of vendors

- **Have an Incident Response and Recovery Plan(s)**
  - Include playbooks for specific responses based on risks. For example:
    - Ransomware
    - Vendor review and removal

- **Conduct Exercises**
  - Technical Exercises for IT team with forensic partners
  - Leadership Exercises on how decisions are made
  - Lessons learned inform policy and incident response and recovery

5 Other Actions to Increase Preparedness and Reduce Liability

- **Consider Cyber Insurance**
  - Ensure adequate coverage – you need to understand your actual risk
  - Ensure you understand what claims are excepted – cybersecurity insurance is changing quickly
  - Ensure compliance with required policies & controls to maintain coverage

- **Engage with third-parties to augment existing capabilities and fill gaps**
  - Information Sharing and Analysis Centers (ISACs)
  - Threat Intelligence – US Cybersecurity and Infrastructure Security Agency (CISA)
  - Incident Response
  - Outside Counsel and Risk Advisors

Finally….

- Remember that cybersecurity risk is organizational risk
- Commitment and support must come from the top
- Your approach must address people, process, and technology
- Recognize that no solution is perfect – attacks and incidents will happen – be ready!

Gracias por su atención

This document is published by the law firm Venable LLP. It is not intended to provide legal advice or opinion. Such advice may only be given when related to specific fact situations that Venable has accepted an engagement as counsel to address.

VENABLE LLP