Information Security Program

Executive Overview

Agenda

- The Case for Information Security
- Information Security Governance
- Next Steps
- Supporting Business Processes

The Case for Information Security

The Case for Information Security

https://www.dhs.gov/be-cyber-smart/facts

The Case for Information Security

Phishing

82

Number of seconds, on average, it takes for a recipient to click on a phishing email, according to a survey from Osterman Research Inc., a market researcher, and security firm IronScales Ltd. They polled 252 security professionals in the U.S. and U.K.

Phishing

$450,000

Amount lost by Frank Krasovec, chairman of Dash Brands Ltd., who owns Domino's Pizza Inc. franchises in China, in a business-email scheme over three days in 2018, The WSJ reports

https://www.wsj.com/pro/cybersecurity

The Case for Information Security

Patching

46%

Percentage of 2,053 organizations that had a cybersecurity incident in the last year attributed to an **unpatched vulnerability**, according to Cisco Systems Inc.'s annual CISO Benchmark Study. That is up from 30% in last year's study.

Internet Of Things

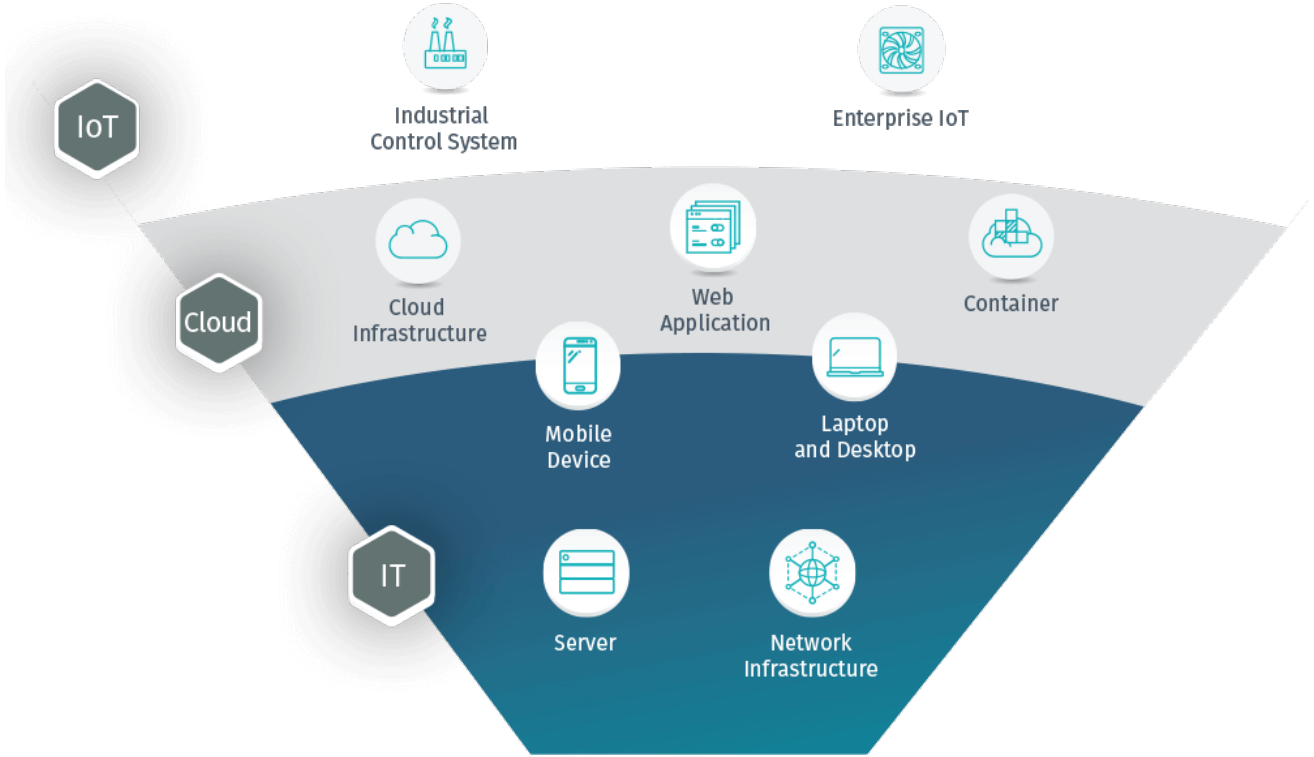
39%

Percentage of organizations that had a security compromise in the last year involving mobile or **Internet-of-Things** devices, according to Verizon, which polled 876 professionals responsible for the devices. In the 2019 study, 33% reported such incidents and in 2018's study, 27%.

https://www.wsj.com/pro/cybersecurity

The Case for Information Security

Attack Surface



https://www.tenable.com/cyber-exposure

The Case for Information Security

Types of Attackers

- Hackers
  - Malicious individuals who attacks computer systems
- Outsiders
  - Attacks launched from the outside by **unauthorized** subject(s) - i.e. “Black Hat Hacker”
- **Insiders**
  - **Intentional** or **Accidental** attack launched from the inside by an **authorized** subject(s)

- Bots and Botnets
  - Computer system running malware controlled via a botnet (Command and Control Network)
- Phishers
  - Malicious attacker who attempts to trick users into divulging sensitive information- i.e. Credentials, PII, etc…
  - Otherwise known as “Social Engineering”

The Case for Information Security

Ad Hoc / Reactive Security

- Results in **Lost Opportunities** as resources are diverted to respond to avoidable events

Governed / Proactive Security

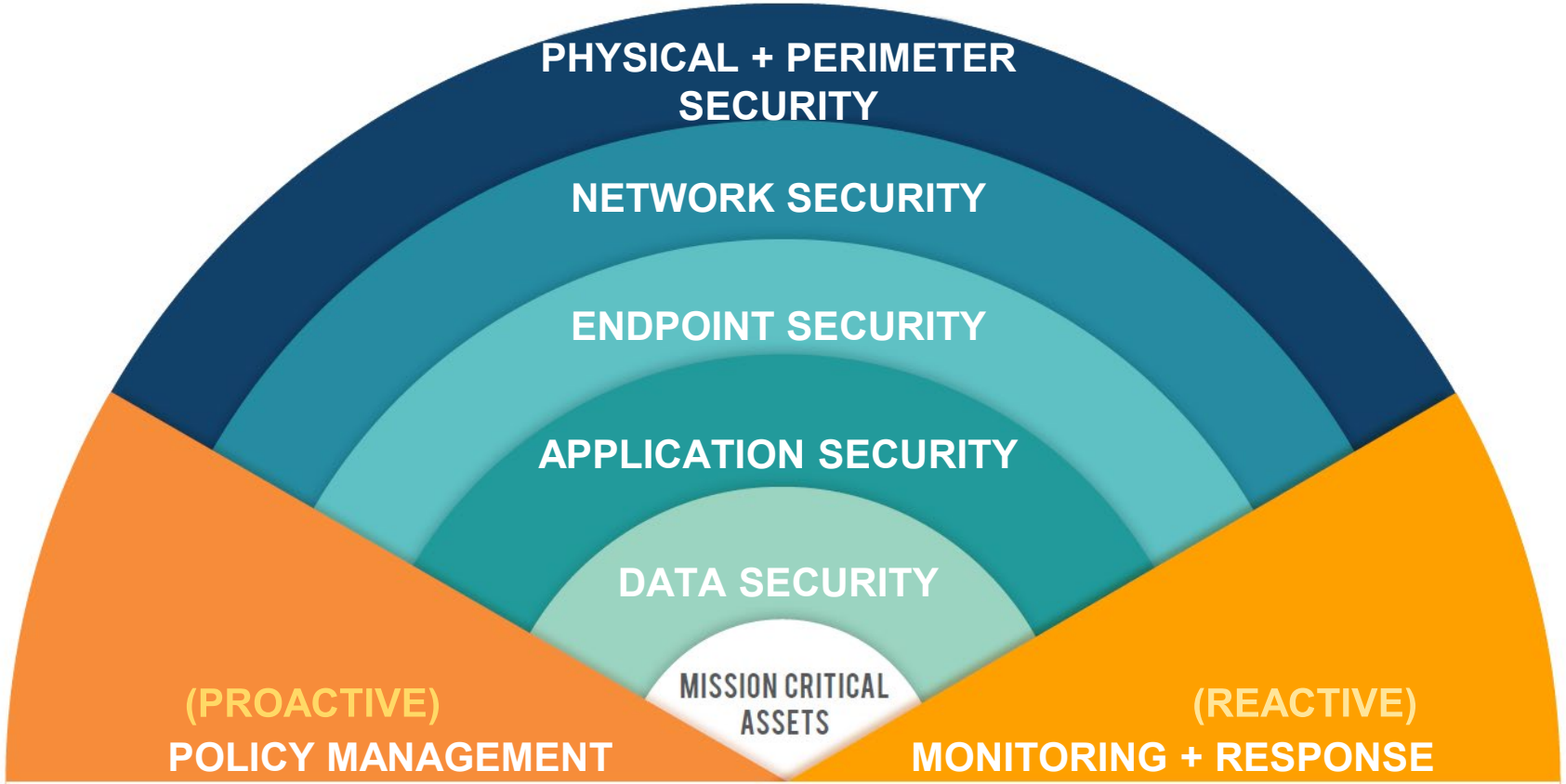
- Reduces the amount of time spent on “Reactive” events
- Allows resources to focus on proactive or other business generating activities

Meeting the Challenge

Core Defenses

- Information Security Governance
  - How we manage our security risks
- Least Privilege
  - Minimum amount of access (Authorization) required to perform job duties
- Need to Know
  - More granular than Least Privilege (Database Read Access vs Row/Record Security)
- Defense in Depth
  - Layered defense applying multiple safeguards (controls) to protect an ASSET!

Defense in Depth (DiD)



Information Governance in Practice

High Risk Attack Vector: Insiders

- Primary Defense: Policies and Procedures
  - Personnel Screening (e.g. background checks)
  - Data Classification (least privilege)
  - **On/Off boarding procedures**
  - Security Awareness Training
- Management + HR + IT = Entire Business
  - Least Privilege (Access required to perform the job)
  - Role Changes (Access updated appropriately : Prevent Permission Creep)
  - Termination - Access removed in a timely and efficient manner
    - Network Access
    - Internal Apps
    - **Cloud Apps** (HR, CRM, etc….)

Information Security Governance

Enterprise Information Security Charter

The Investor Group recognizes that information and IT assets are critical business assets. It is the responsibility of all users to ensure the safeguarding of business assets. The Investor Group requires the company to implement, maintain and monitor a comprehensive **enterprise information security policy** and **compliance program** appropriate to:

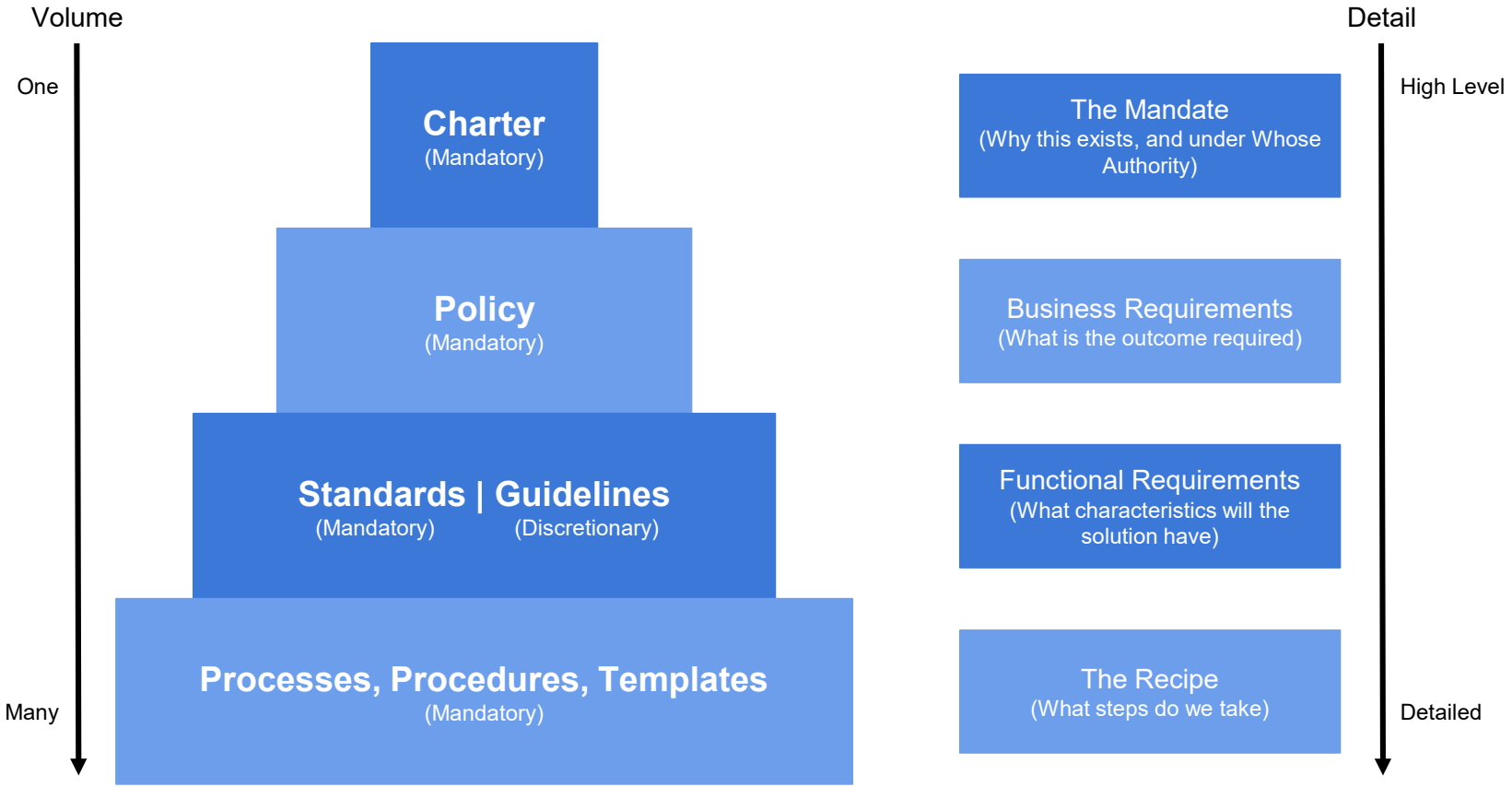
- The risks of the business
- Generally accepted information security practices
- Applicable legal and regulatory requirements

Enterprise Information Security Charter

Executive management:

- Will incorporate cybersecurity requirements into its business planning processes
- Will allocate the resources (people, processes, and technology) required to protect its information systems as part of its capital planning and investment control processes

Information Security Governance



Information Security Policies

The Information Security Policies establish a framework under which the IT organization(s) must operate. These policies are designed to protect the **Confidentiality**, **Integrity**, and **Availability** of the Company's Information Systems.

The IT Department cannot implement and enforce these policies in a vacuum.

Information Security is the responsibility of "ALL" company employees.

Information Security Policies

2021 Policy Revisions

- Aligned Policies with v8 of the CIS Controls
- Condensed 100's of policy statements into 18 distinct best practices
- Consolidated into 5 Policy Documents
    - *IS.01 Information Security Charter* - Outlines the Information Security Program
    - *IS.02 Basic Cyber Hygiene Policy* - CIS Controls that must be implemented regardless of risk.
    - *IS.03 Enhance Cyber Hygiene Policy* - Specific CIS Controls selected to address increased levels of risk and operational complexity.
    - *IS.04 Advanced Cyber Hygiene Policy* - Specific CIS Controls selected to lesson the impact of sophisticated cyber attacks.
    - *IS.05 Cybersecurity Guidelines* - Optional CIS Controls that should be implemented depending business requirements

Information Security Policy Coverage

1. Inventory and Control of Enterprise Assets
2. Inventory and Control of Software Assets
3. Data Protection
4. Secure Configuration of Enterprise Assets and Software
5. Account Management
6. Access Control Management
7. Continuous Vulnerability Management
8. Audit Log Management
9. Email and Web Browser Protections
10. Malware Defenses
11. Data Recovery
12. Network Infrastructure Management
13. Network Monitoring and Defense
14. Security Awareness and Skills Training
15. Service Provider Management
16. Application Software Security
17. Incident Response Management
18. Penetration Testing

Next Steps

Business Leaders

- **IT Security Governance Committee**
  - Create Security Strategy
  - Implement Policies
  - Establish Periodic Security Program Review
  - Promote Security Awareness Training

IT Department

1. **Automate and Test Backups**
2. **Implement Multi-Factor Authentication**
3. **Implement Automatic Software Patching and Vulnerability Management**

IT Department

4. **Top CIS Controls to Prevent a Breach**
   - **#4 Secure Configuration**
   - **#5 Account Management**
   - **#6 Access Control**
   - **#14 Security Awareness Training**
5. **Asset Management**
6. **Implement Basic Cyber Hygiene Policy**
7. **AUTOMATE AS MUCH AS POSSIBLE**

Supporting Business Processes

- Risk Management
  - Business Continuity Planning
  - Business Impact Analysis
- Disaster Recovery Plan
- Incident Response Plan

Questions & Answers