Cybersecurity – Information Security Program Basics

Erwin Martinez, Chief Information Officer
British Columbia Ferry Services, Inc.
September 16, 2019

BCFerries

Topics

- Information Security Mission
- Beliefs and Concepts
- Information Security Principles
- Useful External Frameworks and Reports
- IT Security Program Components
- Cyber Risk Insurance
- Cybersecurity – Metrics Tracking
- Cybersecurity – Common Threats
- Cybersecurity – Emerging Trends

Information Security Mission

- Our responsibility in IT is to have an informed level of confidence that the systems and technology we provide are well controlled, secure, available, and reliable.

Beliefs and Concepts

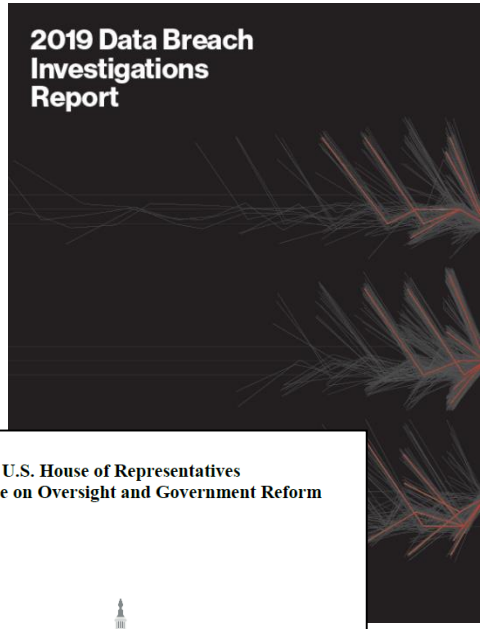
- **Complexity** Information Security Programs are complex, and multi-dimensional; and many organizations get it wrong.
- **Breaches and Failures** Breaches and other information security failures are often the result of mismanagement of areas we (as IT professionals) already know how to manage.
- **IT Ubiquity** Business, government and non-profits are leveraging technology more and more. There is no going back. Every business is an IT business.
- **Frameworks** We are very fortunate in IT to have a large set of frameworks that provide guidance and assistance as we manage IT.
- **Completeness** Completeness is a key concept in cybersecurity. (*Information Security Programs are more like parachutes and less like bologna sandwiches.)* Frameworks can help us deal with completeness.

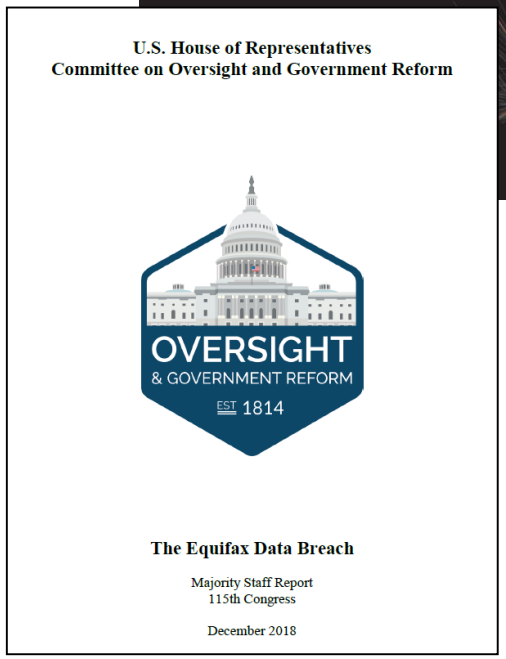
Information Security Principles

- **Defense in depth**
  - No one system is 100% effective, build multiple controls to prevent, detect and slow down attackers
- **Assume breach / Plan for failure**
  - Assume that attackers have already breached your system, and design controls to detect and slow their actions
- **Least privilege**
  - Always design systems and grant access with a least privilege model, only what is needed for the business requirements
- **Risk based**
  - Take a risk based approach when designing controls, continually monitor risk and that controls are balanced in accordance to the organization's risk appetite
- **Security by design / Early involvement**
  - Involvement at early stages of projects and initiatives allows us to build security controls into systems from the beginning

Useful External Frameworks and Reports

- Frameworks
  - ISO 27000 - Information Security
  - NIST Cybersecurity Framework
- Reports
  - Verizon Data Breach Investigations Report
  - U.S. House of Representatives, Committee on Oversight and Government Reform,The Equifax Data Breach, December 2018





ISO 27000 – Information Security

- ISO 27000 standards provide guidance on implementing information security controls and an information security program.
- ISO 27000 series of standards is very robust, composed of 46 separate standards, all on the subject of information security.
  - ISO 27000 — Overview and vocabulary
  - ISO 27001 — Security techniques
  - ISO 27002 — Controls
  - ISO 27003 — Implementation guidance
  - ISO 27004 — Monitoring, measurement, analysis and evaluation
  - ISO 27005 — Risk management

ISO 27000 – Information Security

1. Information security policies
- 1.1 Management direction for information security

2. Organization of information security
- 2.1 Internal organization
- 2.2 Mobile devices and teleworking

3. Human resource security
- 3.1 Prior to employment
- 3.2 During employment
- 3.3 Termination and change of employment

4. Asset management
- 4.1 Responsibility for assets
- 4.2 Information classification
- 4.3 Media handling

5. Access control
- 5.1 Business requirements of access control
- 5.2 User access management
- 5.3 User responsibilities
- 5.4 System and application access control

6. Cryptography
- 6.1 Cryptographic controls

7. Physical and environmental security
- 7.1 Secure areas

8. Operations security
- 8.1 Operational procedures and responsibilities
- 8.2 Protection from malware
- 8.3 Backup
- 8.4 Logging and monitoring
- 8.5 Control of operational
- 8.6 Technical vulnerability management
- 8.7 Information systems audit considerations

9. Communications security
- 9.1 Network security management
- 9.2 Information transfer

10. System acquisition, development and maintenance
- 10.1 Security requirements of information systems
- 10.2 Security in development and support processes
- 10.3 Test data

11. Supplier relationships
- 11.1 Information security in supplier relationships
- 11.2 Supplier service delivery management

12. Information security incident management
- 12.1 Management of information security incidents and improvements

13. Information security aspects of business continuity management
- 13.1 Information security continuity
- 13.2 Redundancies

14. Compliance
- 14.1 Compliance with legal and contractual requirements
- 14.2 Information security reviews

NIST Cybersecurity Framework

- Very robust, lifecycle-based framework

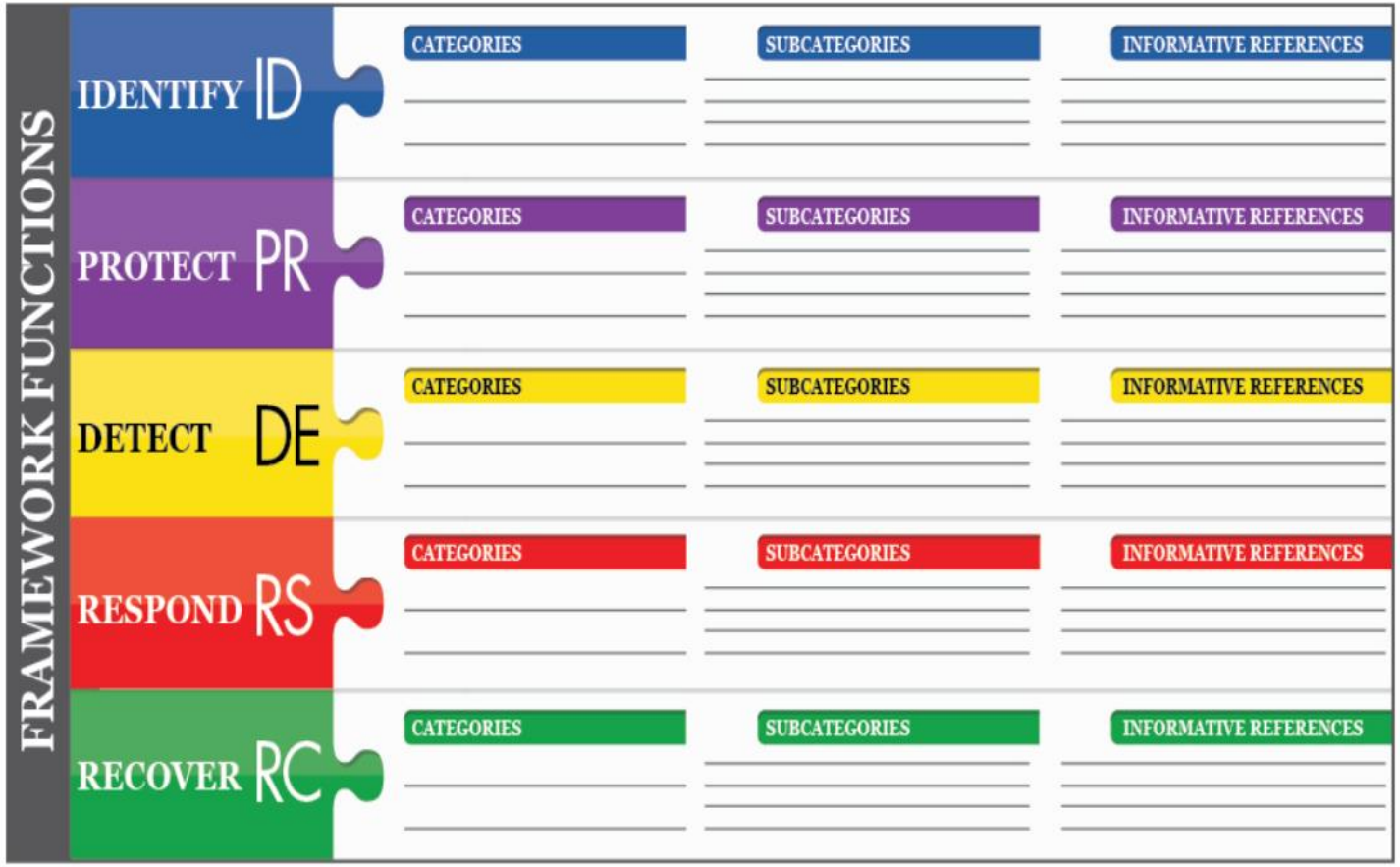


Figure 1: Framework Core Structure

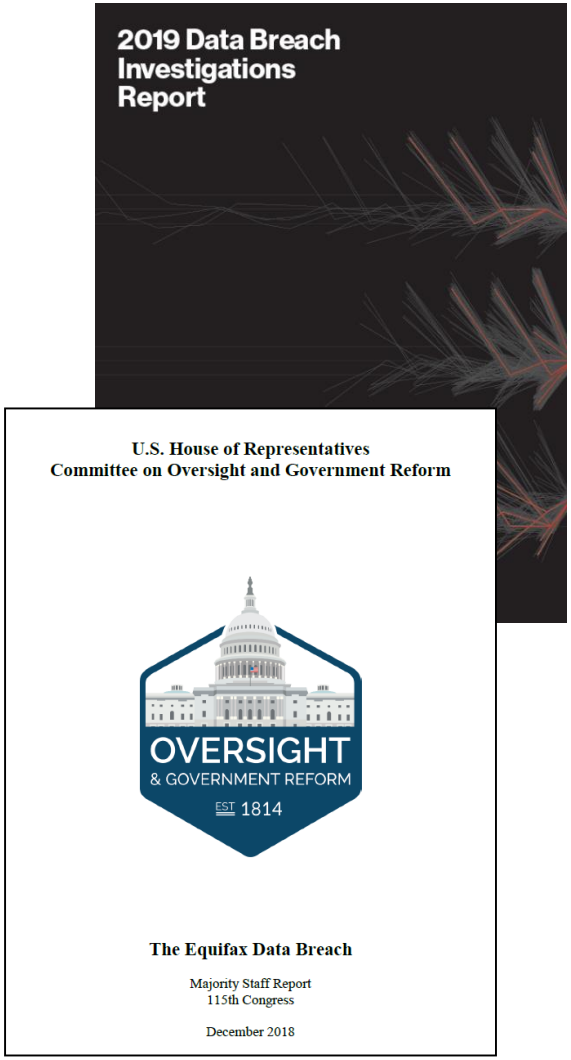
NIST Cybersecurity Framework

Table 2: Function and Category Unique Identifiers

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

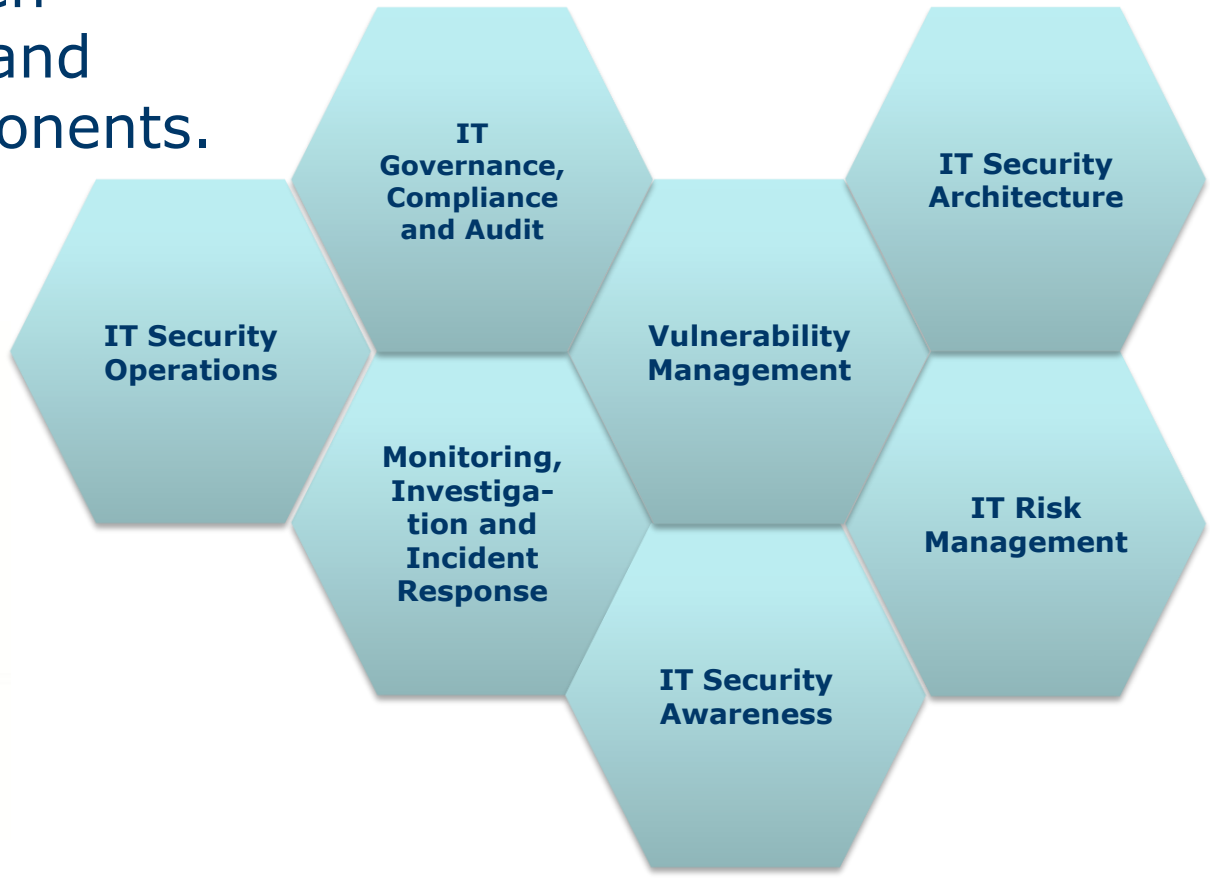
Verizon Data Breach & Report on Equifax Data Breach

- Verizon Data Breach Investigations Report
  - Annual summarization and trend analysis of security events world-wide.
- U.S. House of Representatives, Committee on Oversight and Government Reform, The Equifax Data Breach, December 2018
  - Relatively unique deep dive into an actual cybersecurity breach conducted with the investigative powers of the U.S. Congress.
  - Includes quotes and citations from interviews of Equifax employees.



IT Security Program Components

The IT Security Program is built from seven inter-connected and reinforcing components.



All IT Security Programs are different. Presented here is an example of what one effective program might look like.

Program Component Activities

IT Governance, Compliance and Audit

- Developing policies and standards for IT
- Tracking updates to policies and standards
- COBIT 5 adoption and capability tracking
- Managing IT general controls process
- Process reviews / audits
- Liaison with Internal Audit

IT Security Architecture

- Developing the overall interconnected and layered IT Security defenses
- Advising and overseeing infrastructure and system builds to ensure alignment with IT Security architecture
- Partnered in an empowered role with IT Enterprise Architecture office

IT Security Operations

- Installing, configuring and maintaining IT Security systems
- Ensuring reliable, effective and up-to-date IT security systems
- Managing the roadmap of IT Security systems
- Managing certificate/encryption infrastructure
- Reviewing system hardening and configurations
- Assisting in secure installations, configurations and builds with operational and project teams

Monitoring, Investigation and Incident Response

- Daily monitoring of IT security events and alerts
- Investigation of IT security events and alerts
- Tuning of monitoring systems
- Identification, containment and resolution of IT security incidents
- Threat hunting

Program Component Activities

Vulnerability Management

- Patch management (oversight, advice and direction)
- Penetration testing (external/internal)
- Vulnerability scans and remediation (external/internal)
- Ongoing monitoring of threat and risk landscape
- Risk based evaluation of new threats and risks
- Ad-hoc reviews and configuration reviews

IT Risk Management

- Annual formal and comprehensive IT risk assessment
- Consolidated risk/issue log - tracking to resolution
- Ongoing monitoring of threat and risk landscape
- Involvement in projects:
  - Security Threat Risk Assessment (STRA) process
  - Assisting in design, requirements, architecture
  - Assisting in product/vendor selection

IT Security Awareness

- Providing IT Security Awareness training
- Fostering awareness of IT policies, standards and processes
- Fostering awareness of threats and risks to IT systems
- Phishing testing on a quarterly basis
- Password strength audits on a quarterly basis

Examples of Useful Artifacts

- Information Security Policy
- Information Security Architecture
- Information Security Education Bulletins
- Common Attack Scenarios Analysis
- Security Threat Risk Analysis Process
- External Penetration Test Report
- IT Risk Assessment
- IT General Controls
- Cyber Incident Planning
  - Cyber Incident Response Plans
  - Tabletop Cyber Incident Tests
- Metrics
  - Executive/Board Level Dashboards
  - Detailed Metrics

Cyber Risk Insurance Summary

- Possible Coverage
  - Internet Media Liability
  - Network Security and Privacy Incident
  - Regulatory Proceedings Finds and Penalties
  - Digital Asset Loss
  - Cyber Extortion
  - Business Interruption and Associated Costs
- Triggering Events
  - Unauthorized access, unauthorized use, malicious code, malware, Denial of Service Attack upon company computer systems that result in interruption of service; or
  - Interruption of service actively caused by the company in responding to unauthorized access/use

Whether Cyber Risk Insurance is an appropriate investment for your organization is a complex, risk-benefit decision.

Cybersecurity –Metrics Tracking

- Security Incidents
- Compliance with IT General Controls
- Security Awareness Course Completion
- Phishing Tests and Events
- Patching Statistics
- Vulnerability Scan Results
- Endpoint Protection Stats
- Password Strength Audit Results
- Security Program Calendar of Activities
- IT Risk Assessment – Residual Risk Analysis

Cybersecurity – Common Threats

- Denial of Service (DoS)
- Phishing
- Use of stolen credentials
- Ransomware
- Spyware / Keyloggers
- Pretexting / Social Engineering
- Misconfiguration
- Privilege Abuse (insider threat)
- Hacking / Website Vulnerabilities
- Emailed virus / malware

Cybersecurity – Emerging Trends

- **Cybercrime**
  - Ransomware
  - Social Engineering
  - Internet of Things – expansion of threat surface
  - The Rise of Hacktivism
  - State-sponsored cybercrime
  - Time lag between breach and breach detection
- **Management**
  - Elevation of Chief Information Security Officer (CISO) role
    - CISO as an empowered role
  - Board involvement / board reporting
  - Scarcity of qualified people resources
  - Security firms on retainer

Wrap-up and Q&A