Information Security, Cybersecurity, and Privacy:

An Ounce of Prevention…

Garland Sharratt
Information security consultant
Kelowna

Dec. 4, 2019
FutureBiz Penticton

Overview

- Threats & risks
- Security
- Compliance
- Privacy
- Controls
- Incidents
- Incident response planning
- Frameworks
- Governance

Disclaimer

This presentation is provided for general information purposes only and does not constitute professional advice.

Threats, vulnerabilities, risks, technologies, products, services, etc., change quickly.

No one is responsible for your organization’s security and privacy except you and your organization.

Don’t automatically believe anything you see and hear, even here; that's part of being secure.

Common threats & risks

- Social engineering
  - Phishing, spear ~, vishing
  - Fraudulent emails
  - Bad email links, email attachments, websites
- Bad software, browser extensions
- Device failure, loss, theft
- Website, SaaS compromise
- Admins, employees: actions, sickness, departure
- Suppliers, partners, customers
- Laws: privacy, security breach notification

- Security incidents
  - Account take-over
  - Business email compromise (BEC)
  - Malware infestation
  - Ransomware
  - Data theft, release, modification, loss
  - IT unavailability
  - Production unavailability
- Privacy incidents
  - Personal information theft, release, modification, loss, etc. – employees/customer/etc.
  - Mandatory breach notifications

Common enablers

- Weak passwords
- Reused passwords
- No second-factor authentication (2FA, MFA)
- No data backup
- Insecure devices, networks
- Lack of security awareness training
- No acceptable use policy (AUP)
- No proper oversight of third-parties, suppliers, cloud
- Insecure software development (AppSec)

Information security

- Information security ≈ CIA
  - Confidentiality
  - Integrity: accuracy, authenticity, non-repudiation
  - Availability: up-time, reliability, resilience
- Cybersecurity ≈ Internet security
- Security events caused by threats if enabled by vulnerabilities
  - Controls reduce risk of security events materializing and/or mitigate when they do
- Preventive, Deterrent, Detective, Corrective, Compensating, Recovery
- Administrative, Technical, Physical
- Security and user convenience: choose one – but not always

Information security - 2

- Key security principles
  - Reduce attack surface: Minimize number of things to protect
  - Defense in depth: Multiple layers of security
  - Least privilege: Limit permissions of people
  - Assumption of breach
  - Security by design
- Security scopes
  - IT: device, networks, accounts, ...
  - Production environment (e.g., SaaS): local, cloud; AppSec (OWASP!)
  - Website
  - External: SaaS/cloud, third parties, partners, channels, …
  - Public: social media, …

Compliance types

1. External: Laws and regulations
   - Privacy, data protection: PIPEDA, BC PIPA, etc.
   - Anti-spam: CASL, ...
   - Health data: HIPAA, ...
2. External: Commercial contracts, NDAs, ...
   - From: customer, partners, channels, insurers, …
   - PCI DSS
   - SOC 2, ISO 27001, FedRAMP, ...
3. External: Industry best practices
   - For insurance, etc.
4. Internal: policies, standards, guidelines, procedures
   - External audit: SOC 2, ISO 27001, ...

Security vs. compliance

- Security
  - Protects information from threats using controls
- Compliance
  - A demonstration, report of how the security program meets specific security standards, either internal or external
  - Privacy, etc.
- Security ≠ compliance
  - Good security but poor compliance
  - Good compliance but poor security
- How to be secure vs. How to prove to others you are secure
  - Employees, customers, partners, channels, insurers, regulators, …

https:www.j4vv4d.com/security-vs-compliance-2

Confidential information

- Personal information (PI), personal data
- Business information, Intellectual Property
- Confidentiality agreements
- Scope / whose PI
  - Your employees'
  - Your customers'
  - Your partners', channels', resellers', … (third parties)
  - Maybe your customers' customers'

Privacy & Data Protection

- Good business practice + security + compliance (legal)
- Personally Identifiable Information (PII), Personal Data
- Must identify privacy laws that apply to your organization:
  - PIPEDA – Canada + PIPA - BC
  - California Consumer Privacy Act (CCPA), effective 2020-01-01
  - HIPAA - US - medical
  - EU's General Data Protection Regulation (GDPR) - processing
  - EU's ePrivacy Regulation - transmission
  - ...
- Big set of requirements
- Mandatory breach reporting in some cases
- Big fines
- Privacy by design

Privacy / data protection principles/laws

PIPEDA

1. Accountability
2. Identifying Purposes
3. Consent
4. Limiting Collection
5. Limiting Use, Disclosure, and Retention
6. Accuracy
7. Safeguards
8. Openness
9. Individual Access
10. Challenging Compliance

GDPR

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimization
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality (security)
7. Accountability

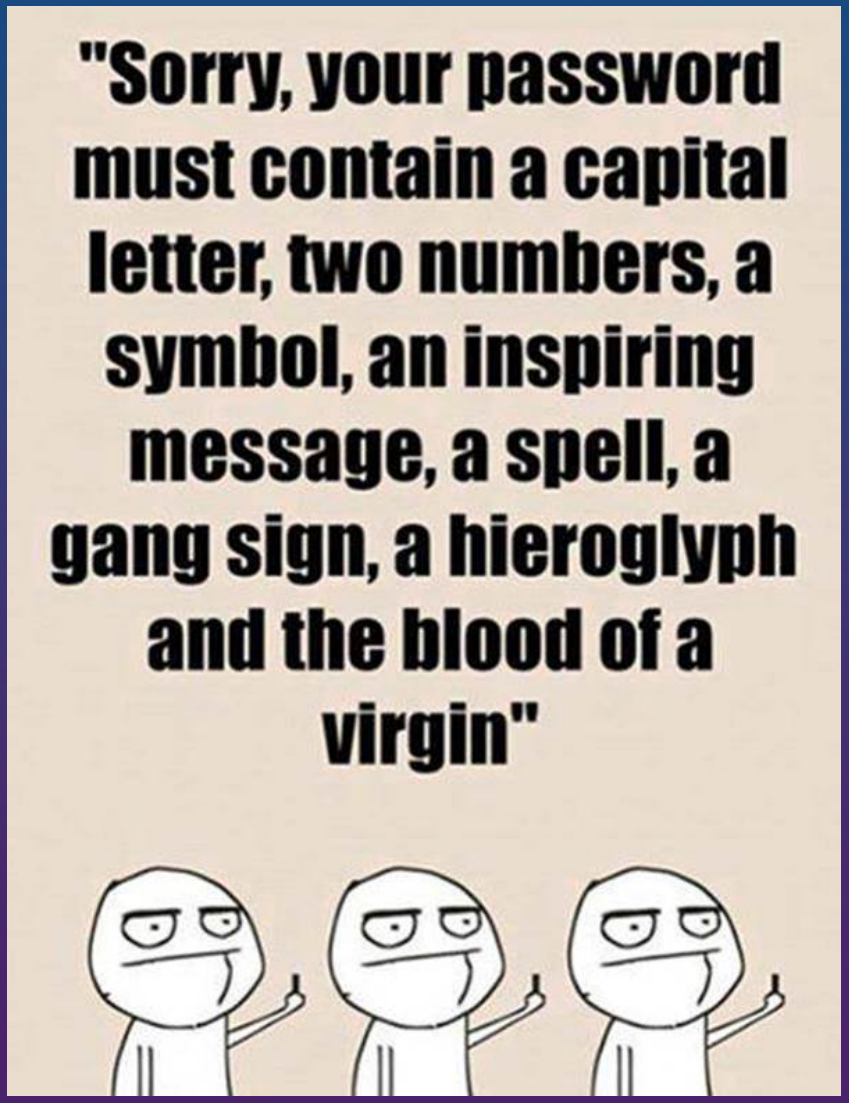
Device security

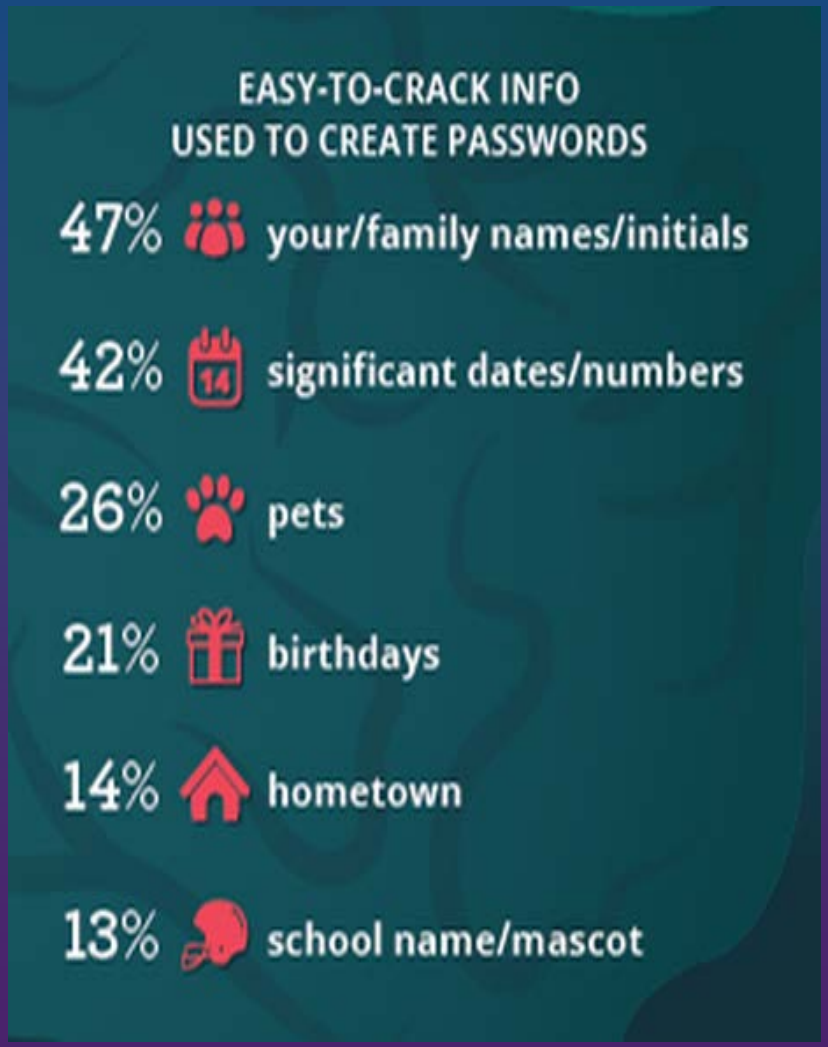
- Strong passwords/PINs
  - mobile: auto-wipe on 10 wrong guesses
- Patch, update OS & application software still supported
  - Stop using H/W & OSs (& applications) no longer getting updates
- Browser privacy extensions against malvertising
  - HTTPS Everywhere + Privacy Badger + uBlock Origin
- Be careful choosing & installing s/w, extensions
- Firewalls: block incoming AMAP
- Routers: WPA2 Personal, Enterprise, block incoming AMAP

Device security- Encryption & backup

- Device full-disk encryption
  - Windows BitLocker, macOS File Vault 2, mobile, ...
- USB drive encryption
  - Windows BitLocker To Go, MacOS Disk Utility, VeraCrypt, ...
- Backup files first to cloud, then locally
  - CrashPlan, Backblaze, …
- System backup:
  - Windows, macOS, Acronis True Image, …

Passwords





https:blog.lastpass.com/2016/09/infographic-introducing-the-psychology-of-passwords.html

Passwords & password managers

- Passwords a huge security risk
  - Phishing, stuffing, spraying, brute forcing, guessing
- "All" passwords must be strong: long (e.g., 20+ chars), random
  - Unique for each account, thing, never reused (Never shared)
  - If you can easily remember it, it's too weak
- Password managers
  - Not: PMs built into browsers, Apple iCloud keychain, etc.
  - LastPass – LogMeIn (Boston) – "LastPass Teams"
  - 1Password – AgileBits (Toronto) – "1Password Teams, Business"
- Start changing passwords beginning with highest risk accounts
  - Email is high priority due to account recovery attack risk
- PMs provide great protection against phishing

Second-factor authentication

- Second factor (2FA), Multi-factor authentication (MFA)
  - Against: phishing, stuffing, spraying, brute forcing, guessing
- Options – best to worst:
  - Hardware dongles
    - U2F, YubiKey, …
  - Push notification
    - Duo Push, …
  - Time-based One Time Password (TOTP) app
    - Authy, Google Authenticator – 6-digit codes
  - Code by email
    - Depends on security of email account
  - Code by SMS or phone call
    - SMS and SIM security are poor

- Start enabling on accounts starting with highest risk accounts

Cloud security

- Cloud flavors
  - Software as a Service, SaaS: Gmail, Dropbox, Workday, ...
  - Platform as a Service, PaaS: Heroku, Google Anthos, ...
  - Infrastructure as a Service, IaaS: AWS, MS Azure, GCP, ...
- Compared to local services
  - Shared responsibility model
  - Less control
  - More resilient
  - Can be more secure
- Big security and privacy impact
- Third party risk management
  - Inventory all cloud services in use
  - Each service: up-front review and ongoing monitoring

People – Security awareness training

- Humans usually weakest link in security
  - One team member with poor practices makes entire org vulnerable
- Annual security awareness training + new employees
  - Overview of threats and risks
  - Safe use of Internet, browsers, email, computers, mobile devices, ...
  - Management of credentials, unique passwords, sharing (or not)
  - Password manager and 2FA, MFA use
- Bonus: Phish users occasionally, e.g., Duo Insight, ...
  - Don't name and shame but do identify best teams
- Provide users with Acceptable Use Policy (AUP)

People – Security culture

- Security is everybody's business
- Build awareness, top-of-mind
  - Monthly security shield award
- Provide education on risks, not blame
- Embed Security in process & thinking
  - Involve Security early in new, changed systems, products, projects
- Build security community
  - Security champions program

Incidents

- Security incident
  - Event that compromises integrity, confidentiality, or availability of an information asset (data or system that processes data)
- Privacy incident
  - Event that involves unauthorized use, access, collection, disclosure, disposal, etc., of regulated data like PI
  - Most privacy incidents are also security incidents
- Data breach
  - A privacy incident that meets specific legal definitions
  - Required notification to affected individuals and/or regulatory agencies
  - Contractual obligations may require notice to business clients
- PIPEDA notification obligations for breaches of PI – Nov. 2018
  - Must notify individuals & Privacy Commissioner if “the breach creates a real risk of significant harm to the individual”

Incident response planning

- Assumption of breach
- Incident response plan
- Run regular practices and simulations of incident response plan with all incident response team members

- Cyber insurance, cyber privacy insurance

- Disaster recovery plan
  - Technical part of business continuity plan

Incident response plan

- Identify levels of severity and criteria for invoking the plan
  - Response actions by severity level, escalation triggers
- Identify incident response team and their individual roles
  - Identify training required and provide it
- Identify how to preserve forensic evidence
- Identify external resources, experts you can call on
- Identify who externally might need to be contacted, esp. privacy regulatory bodies, media
- Write canned playbooks for known threats, risks
- Identify post-mortem analyses required

Risk management process

- Do security and privacy threat and risk assessment
  - Including gap analysis against recognized infosec framework: CIS Controls, NIST CSF, ISO 27000
- Then remediate the risks identified, starting with highest risks

1. "Determine" organization's risk tolerance
2. Identify and characterize threats (external): threat modeling, data flow diagrams, ...
3. Assess vulnerability of key assets (internal) to specific threats
4. Determine the risk = likelihood x impact → risk level matrix
5. Identify ways to reduce those risks (mitigations): Accept, reduce, compensate, transfer, share, avoid
6. Prioritize risk reduction measures
7. Implement
8. Check and correct

Likelihood \ Impact	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low Med	Medium	Med Hi	High	High
Likely	Low	Low Med	Medium	Med Hi	High
Possible	Low	Low Med	Medium	Med Hi	Med Hi
Unlikely	Low	Low Med	Low Med	Medium	Med Hi
Very Unlikely	Low	Low	Low Med	Medium	Medium

https:www.thereliabilityblog.com/2017/09/13/beyond-the-risk-matrix

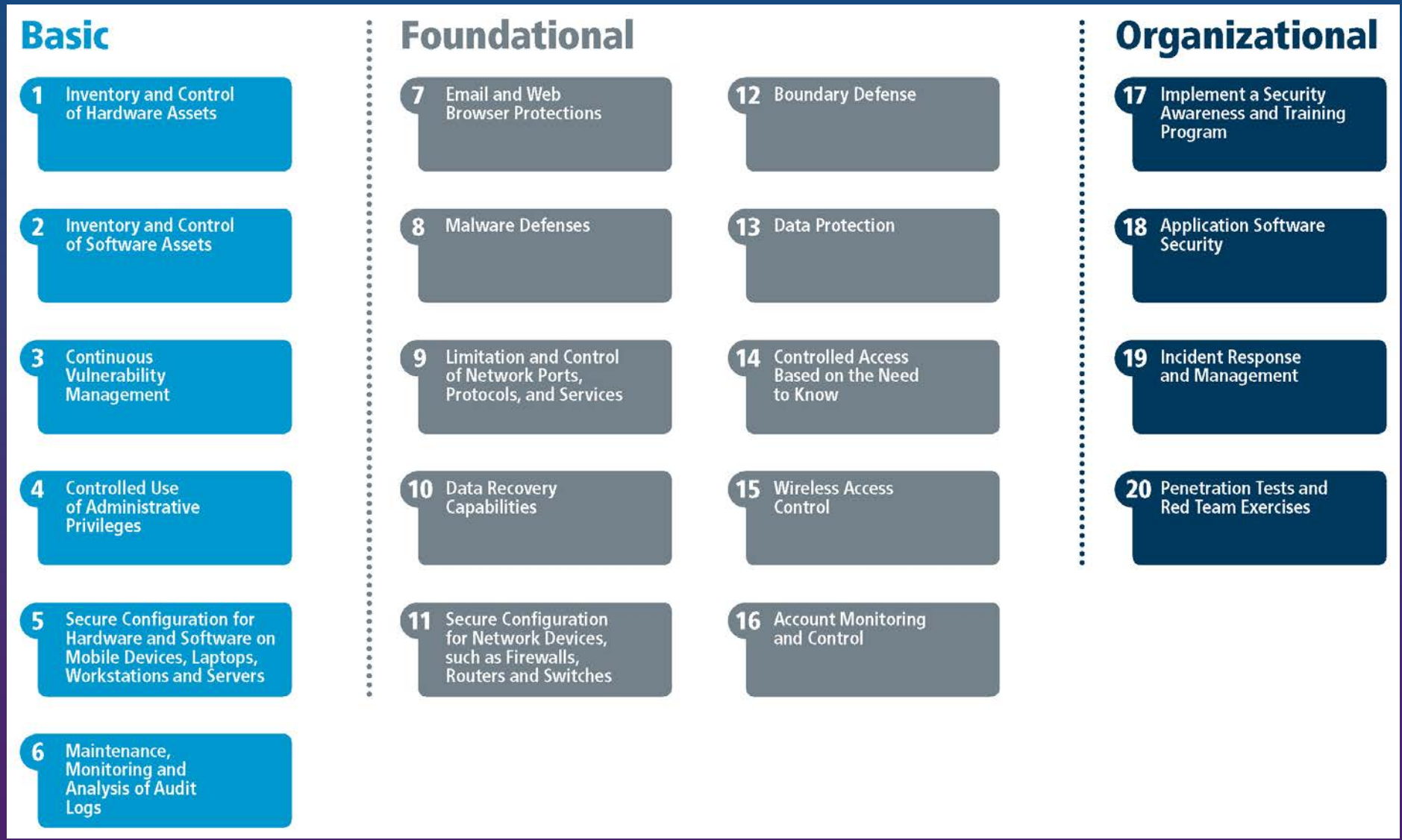
Security frameworks

- **Center for Internet Security (CIS) Controls**
- Canadian Centre for Cyber Security: Baseline Cyber Security Controls for Small and Medium Orgs
  - https:cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations
- Cyber Readiness Institute: Cyber Readiness Program
  - https:www.cyberreadinessinstitute.org/the-cyber-readiness-program
- NIST Cybersecurity Framework (CSF)
- **ISO 27002: best practices for controls**
- ISO 27001: requirements for infosec mgt. system

Framework – ISO 27002 Standard

5. Information security policies
6. Organization of information security
7. Human resource security
8. Asset management
9. Access control
10. Cryptography
11. Physical and environmental security
12. Operations security
13. Communications security
14. System acquisition, development and maintenance
15. Supplier relationships
16. Information security incident management
17. Information security aspects of business continuity management
18. Compliance

Framework - CIS Controls



Framework - CIS Controls – IGs

Implementation Group 3
A mature organization with significant resources and cybersecurity experience to allocate to Sub-Controls

Implementation Group 2
An organization with moderate resources and cybersecurity expertise to implement Sub-Controls

Implementation Group 1
An organization with limited resources and cybersecurity expertise available to implement Sub-Controls

Definitions	1	2	3
Implementation Group 1 CIS Sub-Controls for small, commercial off-the-shelf or home office software environments where sensitivity of the data is low will typically fall under IG1. Remember, any IG1 steps should also be followed by organizations in IG2 and IG3.	●		
Implementation Group 2 CIS Sub-Controls focused on helping security teams manage sensitive client or company information fall under IG2. IG2 steps should also be followed by organizations in IG3.	●	●	
Implementation Group 3 CIS Sub-Controls that reduce the impact of zero-day attacks and targeted attacks from sophisticated adversaries typically fall into IG3. IG1 and IG2 organizations may be unable to implement all IG3 Sub-Controls.	●	●	●

Framework - CIS Controls – 1 of 20

CIS Control 1: Inventory and Control of Hardware Assets

Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	Implementation Groups		
					1	2	3
1.1	Devices	Identify	Utilize an Active Discovery Tool	Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory.		●	●
1.2	Devices	Identify	Use a Passive Asset Discovery Tool	Utilize a passive discovery tool to identify devices connected to the organization's network and automatically update the organization's hardware asset inventory.			●
1.3	Devices	Identify	Use DHCP Logging to Update Asset Inventory	Use Dynamic Host Configuration Protocol (DHCP) logging on all DHCP servers or IP address management tools to update the organization's hardware asset inventory.		●	●
1.4	Devices	Identify	Maintain Detailed Asset Inventory	Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all assets, whether connected to the organization's network or not.	●	●	●
1.5	Devices	Identify	Maintain Asset Inventory Information	Ensure that the hardware asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network.		●	●
1.6	Devices	Respond	Address Unauthorized Assets	Ensure that unauthorized assets are either removed from the network, quarantined or the inventory is updated in a timely manner.	●	●	●
1.7	Devices	Protect	Deploy Port Level Access Control	Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.		●	●
1.8	Devices	Protect	Utilize Client Certificates to Authenticate Hardware Assets	Use client certificates to authenticate hardware assets connecting to the organization's trusted network.			●

Resources 1/3

- Organizations
  - **Okanagan Information Security Group (OISG)**
    - monthly meetings, currently Kelowna
  - **Vancouver Security Special Interest Group (SecSIG)**
    - Slack, monthly mtgs
  - MARS
    - Slack, monthly socials
  - **BC AWARE Day (Jan. 21)**
  - **BSides Vancouver (Mar. 22-24)**
- Other
  - Kelowna Tech Slack > #infosec channel; Kelowna Tech Slack > #privacy channel

Resources 2/3

- GOC - Protecting your business: https://canada.ca/en/services/business/protecting.html
- Canadian Centre for Cyber Security
  - https://cyber.gc.ca/en/information-guidance
- CyberSecure Canada (federal cyber certification program)
  - https://www.ic.gc.ca/eic/site/137.nsf/eng/h_00000.html
- Template for Small Business Information Security Awareness and Training Policy
  - https://www.peerlyst.com/posts/free-resource-template-for-small-business-information-security-awareness-and-training-policy-alan-watkins

Resources 3/3

- **Blogs**
  - https://www.google.com/search?q="information+security"+blog
  - (NewsBlur: free news reader, RSS/Atom)
- Courses
- Books
  - **CISSP BOK, CISM BOK, ...**
- Certifications - generic
  - **CISSP, CISM, ...**
  - CIPP/E, /C, ...
  - CEH, OSCP, ...
- Certifications - tech specific
  - Cisco CCNA, Microsoft, ...
  - AWS, MS Azure, Google Cloud, ...

Governance

- People, Processes, Technology
  - *If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.* – Bruce Schneier
- Top-down support for security, “tone from the top”
- Give someone responsibility for security and technical (non-legal) aspects of privacy
  - Suitable knowledge, interest, influence; don't need to be an expert
  - Believe in and will create a strong security culture
- Define the org’s security program
- Write security policies to govern all org and employee activity
  - ISO 27002 as framework
- Draw heavily on industry security frameworks
- Maturity model: Initial, Repeatable, Defined, Capable, Efficient

TL;DR

- Make someone responsible for security & technical privacy
- Implement technical security measures
  - Update/patch device OSs & applications
  - Back up data: first to cloud, then locally (encrypted)
  - Password manager + Stop reusing passwords +
    Change passwords to long unique, starting with important accounts
  - 2FA, MFA, preferably Google Authenticator type, not SMS
  - Full-disk encryption on devices
- Set up security awareness training program + Drive security culture
- Prepare incident response plan and practice it
- Privacy compliance: start with inventory of all PI, in-house and cloud
- Start working through CIS Controls Implementation Group 1

Garland Sharratt – garland.sharratt@gmail.com