2019 Security 101: an overview of security fundamentals and practice

Technology is everywhere

In 2018, the technology industry sold ...

- **259 million** personal computers[1]
- **1.4 billion** smartphones[2]
- **174 million** tablets[3]
- **11.2 million** servers[4]

77% of enterprises use at least one cloud app.[5]

30% of IT budgets devoted to cloud computing.[5]

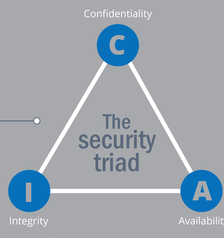
More technology = more threats[6]

- **1 in 3 web requests** leads to malware
- **92% increase** in downloader malware
- **55% increase** in spam volume
- **46% increase** in ransomware threats
- **600% increase** in Internet of Things attacks
- **54% increase** in mobile malware variants

Invincibility is impossible

Perfect security is a practical impossibility; technology is too complex. The goal of security is to mitigate risk as much as possible within reason, keeping system usability and cost in mind.

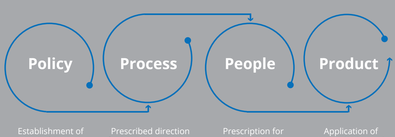
The security triad



The goal of security is to ensure data and system:

- **Confidentiality** (nondisclosure to unauthorized users)
- **Integrity** (true and uncorrupted)
- **Availability** (accessible and functional when needed)

Security is a process, not a product



Policy — Establishment of acceptable uses, security and data integrity standards, and performance expectations

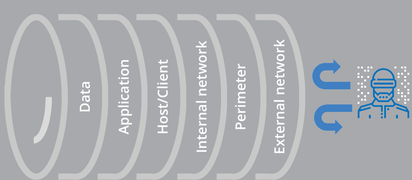
Process — Prescribed direction for how security team and organization should execute security policies and incident response

People — Prescription for establishing security roles and responsibilities of users in an organization

Product — Application of technologies and services designed to safeguard IT assets, infrastructure, applications and data wherever they reside

Layered security = defense in depth

Defense in depth is about layering security to increase the difficulty of a successful breach. If one layer doesn't detect and stop an attack, another layer will.



Data
- Encryption
- Access controls
- Backup
- Pentesting
- Vulnerability scans

Application
- Content filtering
- Auditing
- Data validation
- SSO
- Pentesting
- Vulnerability scans

Host and client
- Authentication
- Antivirus
- Firewalls
- IDS/IPS
- Password hashing
- Logging
- Auditing
- Access controls
- Backup
- Pentesting
- Vulnerability scans

Internal network
- IDS/IPS
- Segmentation
- Logging
- Auditing
- Pentesting
- Vulnerability scans

Perimeter
- Firewalls
- Proxies
- Logging
- Auditing
- Pentesting
- Vulnerability scans

External network
- VPNs
- DMZ
- Logging
- Auditing
- Pentesting
- Vulnerability scans

Calculating risk

Security isn't an absolute; it's about applying appropriate protection based on risk exposure. Calculating risk is a matter of taking four fundamentals into account.

Risk	Threats	Vulnerabilities	Value	Time
Risk exposure that requires security countermeasures	Totality of hacker, malware and user threats facing an organization	Assessment of known and unknown IT system vulnerabilities	Total financial impact of, or loss resulting from, a breach	Amount of time required to successfully penetrate security measures

Types of security controls

Mitigating risk and applying security measures require a system of controls over IT systems and applications. Security comprises three basic control types:

Technical controls: Controls that apply a technology solution to reduce vulnerabilities and mitigate risk. Examples are antivirus software, firewalls, IDS/IPS and encryption.

Management controls: These controls apply security assessment and planning activities to deliver ongoing reduction of risk exposure. Examples include penetration tests, risk and vulnerability assessments, and threat modeling.

Operational controls: These are controls delivered via the day-to-day operations of the security team or the security service provider. Asset inventories, data classification, security awareness training, configuration and change management, and BCDR protocols are all examples.

Getting more secure

Security is dynamic. Providing security products, services and support requires continuous learning and skill building. Look for more guidance on security best practices through Ingram Micro's Security Practice Builder.

[1] Source: IDC
[2] Source: Gartner
[3] Source: Strategy Analytics
[4] Source: IDC
[5] Source: RightScale
[6] Source: Symantec