Los Angeles Chapter
ISSA
Information Systems Security Association

Enterprise Cybersecurity: Building an Effective Defense

Chris Williams

Scott Donaldson

Abdul Aslam

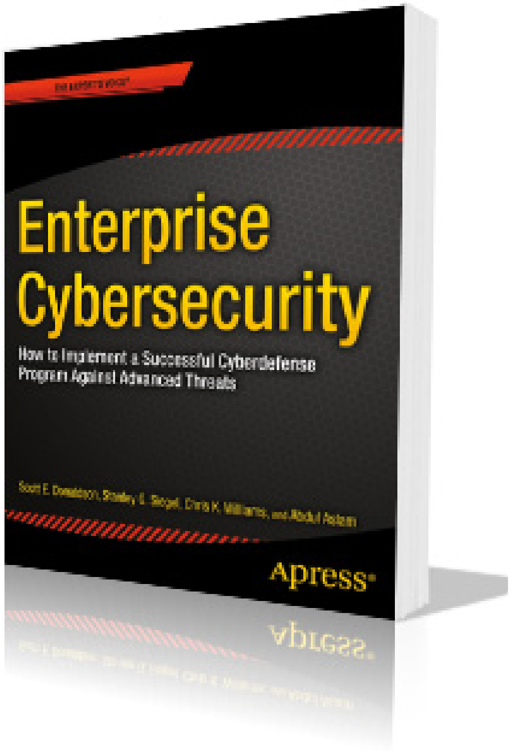
About the Presenters

Co-Authors of *Enterprise Cybersecurity: How to Implement a Successful Cyberdefense Program Against Advanced Threats*

- **Scott E. Donaldson** is a Senior Vice President for Leidos, Inc., a Fortune 500® company that provides scientific, engineering, systems integration, and technical services. He is the Chief Technology Officer (CTO) and IT Director for its Heath and Engineering Sector.

- **Chris K. Williams** is an Enterprise Cybersecurity Architect at Leidos, Inc. He has been designing, deploying, and operating cybersecurity solutions for government and commercial clients for over 20 years, and holds a patent for e-commerce technology.

- **Abdul Aslam** is the Director of Cyber Security Compliance and Risk Management for Leidos, Inc. He has 19 years of experience in devising risk acceptance and compliance frameworks, application security, security operations and information protection.


Enterprise Cybersecurity
How to Implement a Successful Cyberdefense Program Against Advanced Threats
Scott E. Donaldson, Stanley G. Siegel, Chris K. Williams, and Abdul Aslam
Apress

Agenda

1. How you were taught to do cyber defense in the past
2. What modern attackers do to defeat your defenses: the illusion of “defense in depth”
3. Why the defense methods you were taught in the past don’t work against today’s attackers
4. Why the frameworks you’re supposed to implement may not be helpful
5. What you can do that *does* work
6. What you can expect in the future

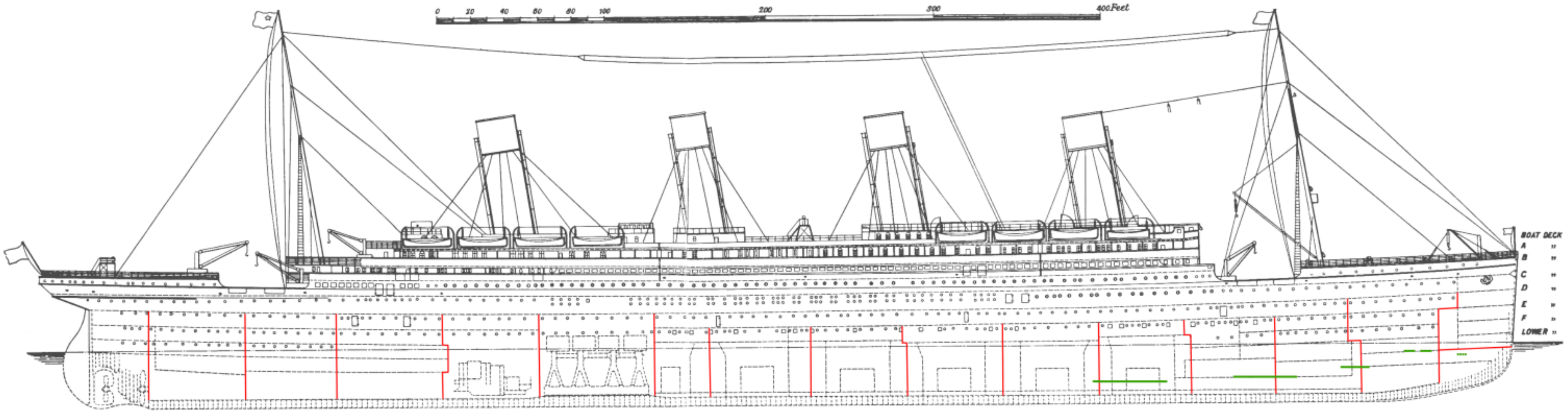
1. “Legacy” Cyberdefense

- ***In the 1990s:***
  - Cyberdefense involved hardening Internet-connected computers against attack.
- ***In the 2000s:***
  - Cyberdefense involved building network perimeters to protect enterprise networks from the Internet.
- ***In the 2010s:***
  - Cyberdefense is struggling to find a new paradigm for protection.

2. The Illusion of "Defense in Depth"

Complexity does not correlate with effectiveness:

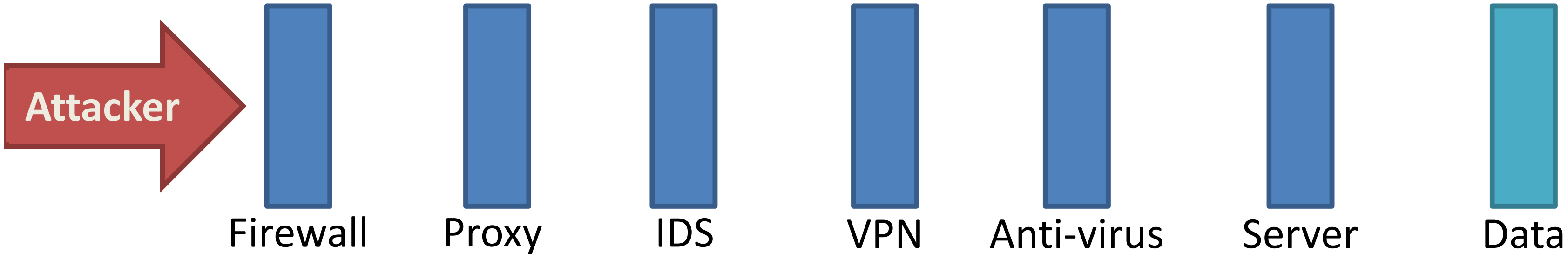
- You think your security is pretty good
- You deploy sophisticated cybersecurity technologies
- Yet you still get pwned



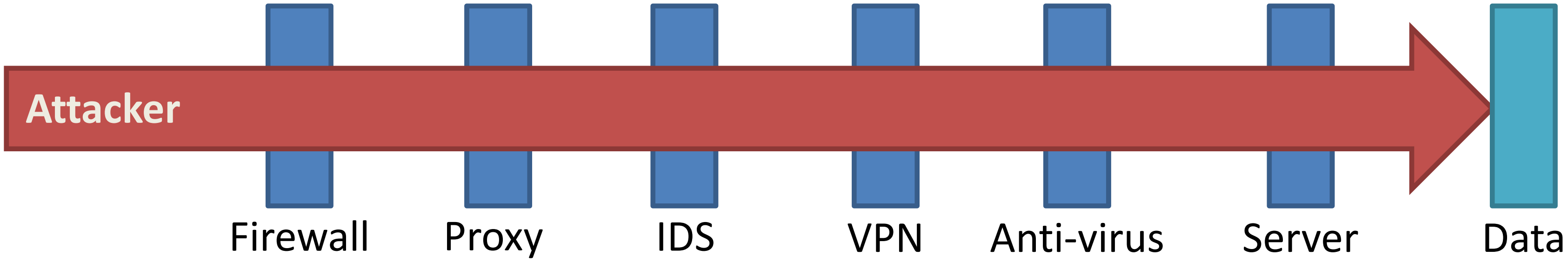
Perhaps your "defense in depth" is not as deep as you think.

“Defense in Depth:” Servers

“Defense in Depth” for servers - the myth:



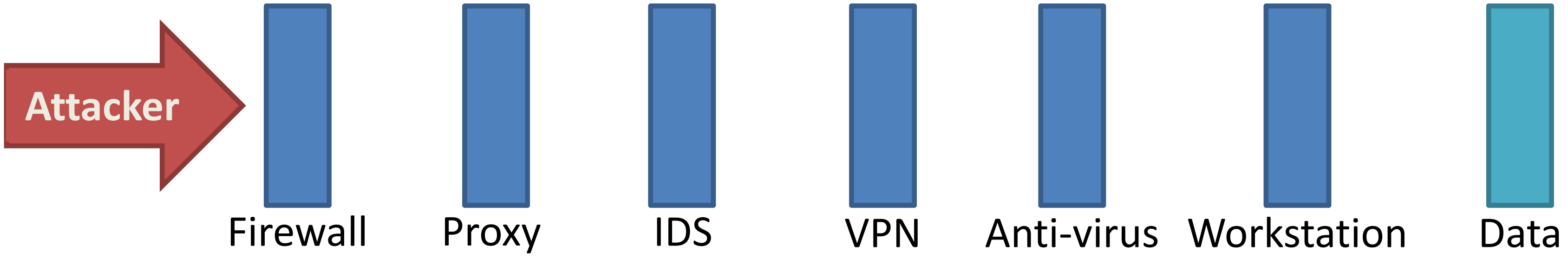
“Defense in Depth” reality with valid admin credentials:



IDS = intrusion detection system   VPN = virtual private network

“Defense in Depth:” Endpoints

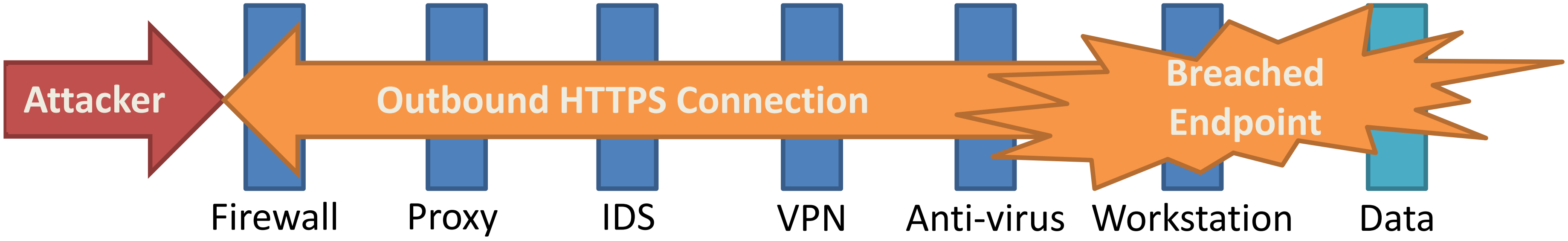
“Defense in Depth” for endpoints - the myth:



Attacker

Firewall Proxy IDS VPN Anti-virus Workstation Data

“Defense in Depth” reality with phishing:



Attacker

Outbound HTTPS Connection

Breached Endpoint

Firewall Proxy IDS VPN Anti-virus Workstation Data

IDS = intrusion detection system VPN = virtual private network

3. Why Cyberdefenses Don’t Work

In a complex environment:

- Flaws are inevitable
- Systems malfunction
- People make mistakes

Therefore:

- Attackers can always gain a foothold, eventually
- Defenders don’t detect the attackers on the inside
- Attackers eventually succeed

Show me artifacts that indicate your defenses catch and stop the attacks that are occurring.

Inevitable Failure: Endpoints

The reality is that endpoints are *always* compromised:

Home PCs

1 / 10

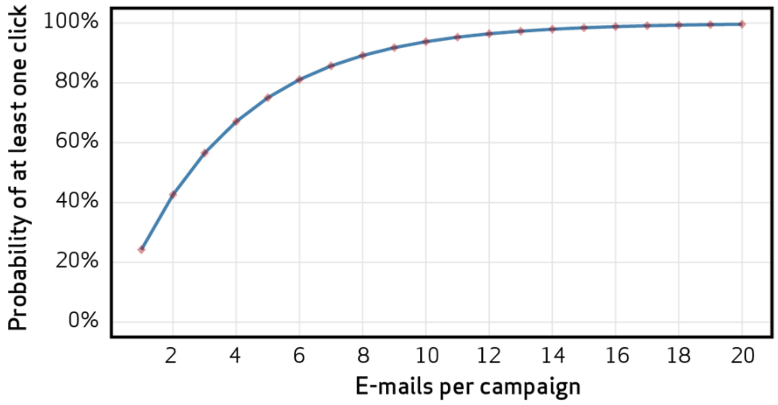
Enterprise PCs

1 / 100

Enterprise Servers

1 / 1,000

One cause is the "Inevitability of the Click":

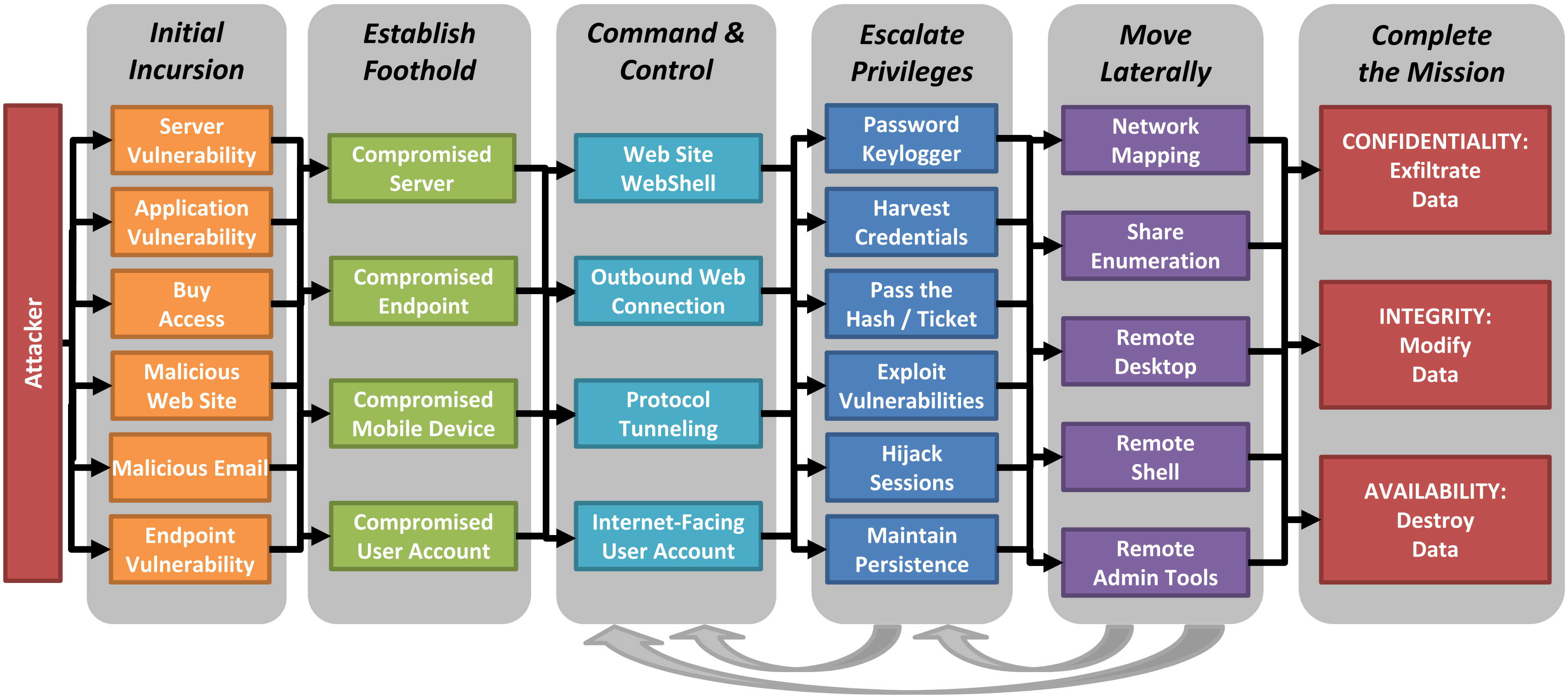


Source: Verizon
2013 Data Breach
Investigations Report

You can reduce these numbers but you CANNOT eliminate them.
Therefore, are you detecting them when they occur?

Anatomy of a Targeted Attack

Targeted attacks methodically work through victim defenses…



Attacker

Initial Incursion

- Server Vulnerability
- Application Vulnerability
- Buy Access
- Malicious Web Site
- Malicious Email
- Endpoint Vulnerability

Establish Foothold

- Compromised Server
- Compromised Endpoint
- Compromised Mobile Device
- Compromised User Account

Command & Control

- Web Site WebShell
- Outbound Web Connection
- Protocol Tunneling
- Internet-Facing User Account

Escalate Privileges

- Password Keylogger
- Harvest Credentials
- Pass the Hash / Ticket
- Exploit Vulnerabilities
- Hijack Sessions
- Maintain Persistence

Move Laterally

- Network Mapping
- Share Enumeration
- Remote Desktop
- Remote Shell
- Remote Admin Tools

Complete the Mission

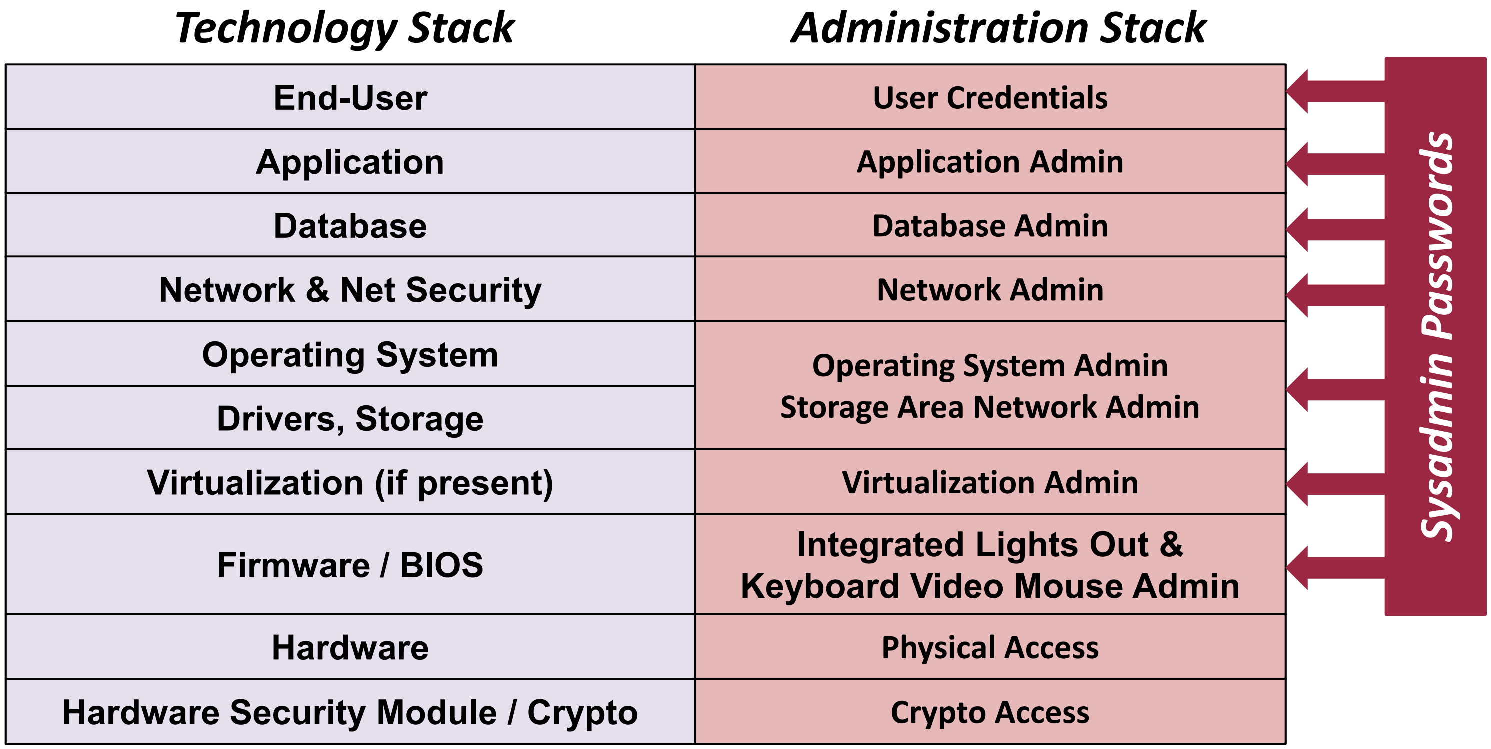
- CONFIDENTIALITY: Exfiltrate Data
- INTEGRITY: Modify Data
- AVAILABILITY: Destroy Data

The sequence gives defenders opportunities to succeed…

The Vulnerability of Systems Administration

Systems Administration channels are the “Achilles Heel”:

- In the datacenter, technologies are stacked and interdependent
- Usually, administrator credentials are just passwords on the network
- Attackers can go “lower in the stack” and bypass upper security layers
- Don’t need to exploit a vulnerability if you can steal the administrator credentials



Technology Stack	*Administration Stack*
End-User	User Credentials
Application	Application Admin
Database	Database Admin
Network & Net Security	Network Admin
Operating System	Operating System Admin Storage Area Network Admin
Drivers, Storage	
Virtualization (if present)	Virtualization Admin
Firmware / BIOS	Integrated Lights Out & Keyboard Video Mouse Admin
Hardware	Physical Access
Hardware Security Module / Crypto	Crypto Access

“Broken Windows”

Windows is the most popular enterprise network operating system:

- Numerous protocol vulnerabilities
  - Pass-the-Hash, Pass-the-Ticket
  - “Gold” and “Silver” tickets
  - Cached credentials
  - Local administrator accounts
- Frequent patches to exploits
- Zero-Day attacks

U.S.
CYBERSECURITY
STOP
Lisa ©2015 6-9 Dist. by WashPostWritersGroup

“Prevention” alone may not be adequate

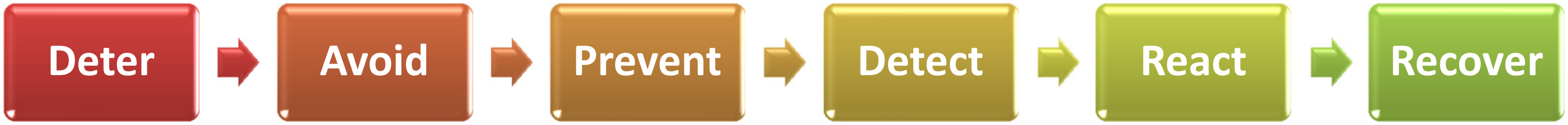
4. The Challenge With Frameworks

- **Major frameworks focus primarily on prevention:**
  - ISO 27001
  - NIST SP800-53
  - SANS / CSC 20
  - PCI
- **“NIST New Framework” of 2013:**
  - Organized around the incident life cycle
  - Unclear how to use it in a cybersecurity program
  - Adoption is not widespread

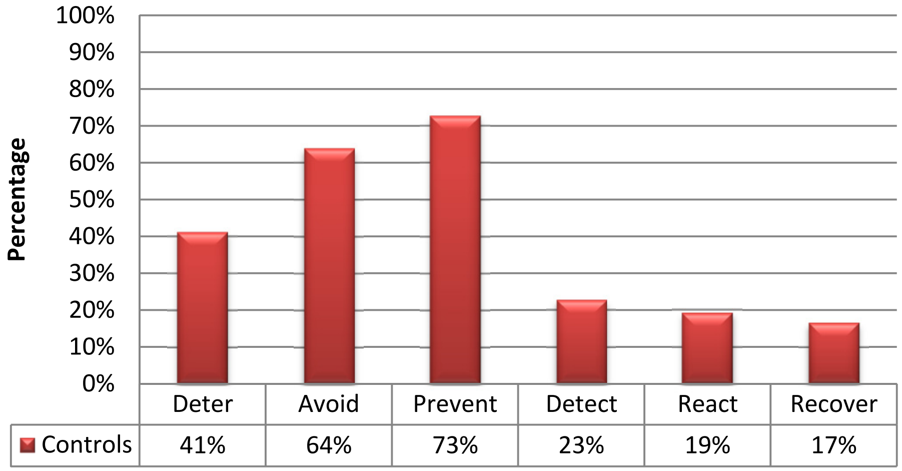
Most frameworks would rather try to prevent attacks.
Few consider how (in)effective that prevention actually is.
Show me artifacts that indicate your prevention is working.

Framework Example: ISO 27001

Consider the Incident Life Cycle:



ISO 27001/2: 114 Total Controls



	Deter	Avoid	Prevent	Detect	React	Recover
🟥 Controls	41%	64%	73%	23%	19%	17%

Data from www.iso27001security.com

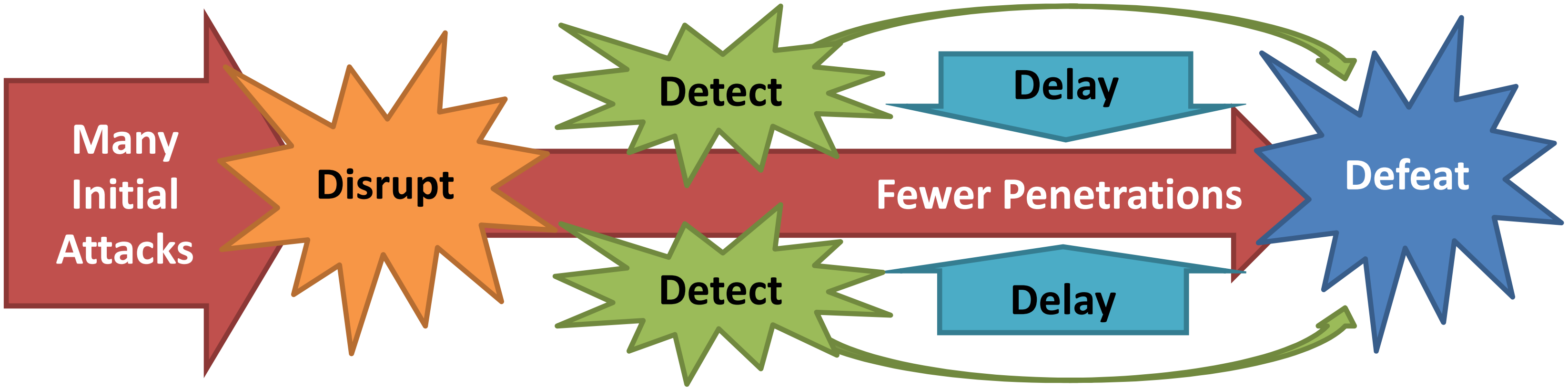
Most ISO 27001 controls focus on deterrence, avoidance, and prevention

Few controls focus on detection, reaction, or recovery.

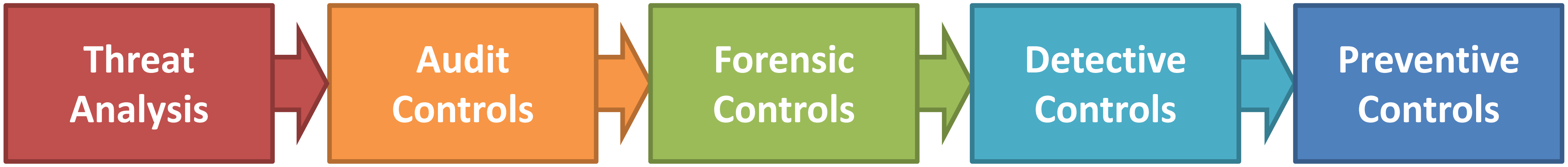
5. A Pragmatic Approach

- **Rather than strive for “perfection,” strive for “good enough:”**
  - Focus on real-world attacks that are most likely to occur
  - Repel attacks when they occur, then improve defenses

- **Design defenses to impede the attack:**
  - Disrupt
  - Detect
  - Delay
  - Defeat



Pragmatic Security: Audit First



Threat Analysis

Audit Controls

Forensic Controls

Detective Controls

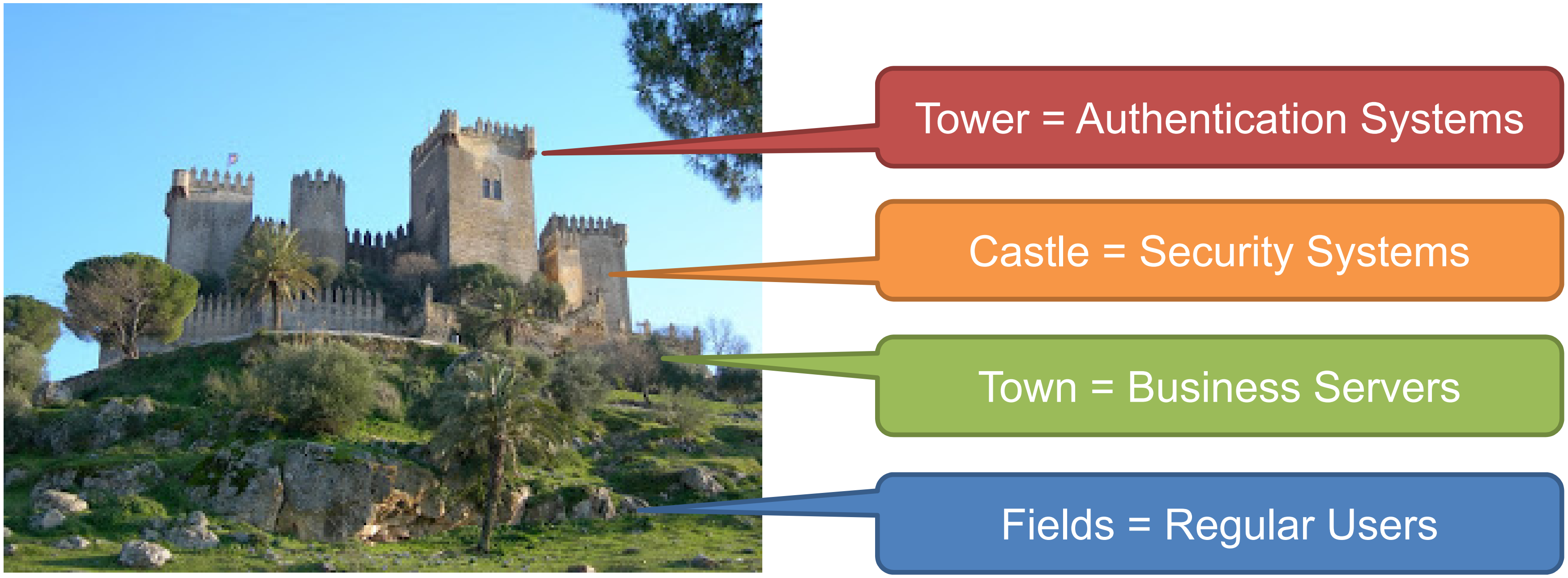
Preventive Controls

- **Don’t try to protect everything**
- **Design Security Around the Threats:**
  - How do you search for the threat?
  - What logs do you need to detect the threat?
  - Can you alert when the threat occurs?
  - Can you block the threat so it does not succeed?

Pragmatic Security: Cyber Castles

We can learn from history by looking at medieval towns:

- Most of the productivity is in the undefended fields and village
- The town is lightly defended, but the castle is heavily defended
- To take the town, you have to control the castle



Tower = Authentication Systems

Castle = Security Systems

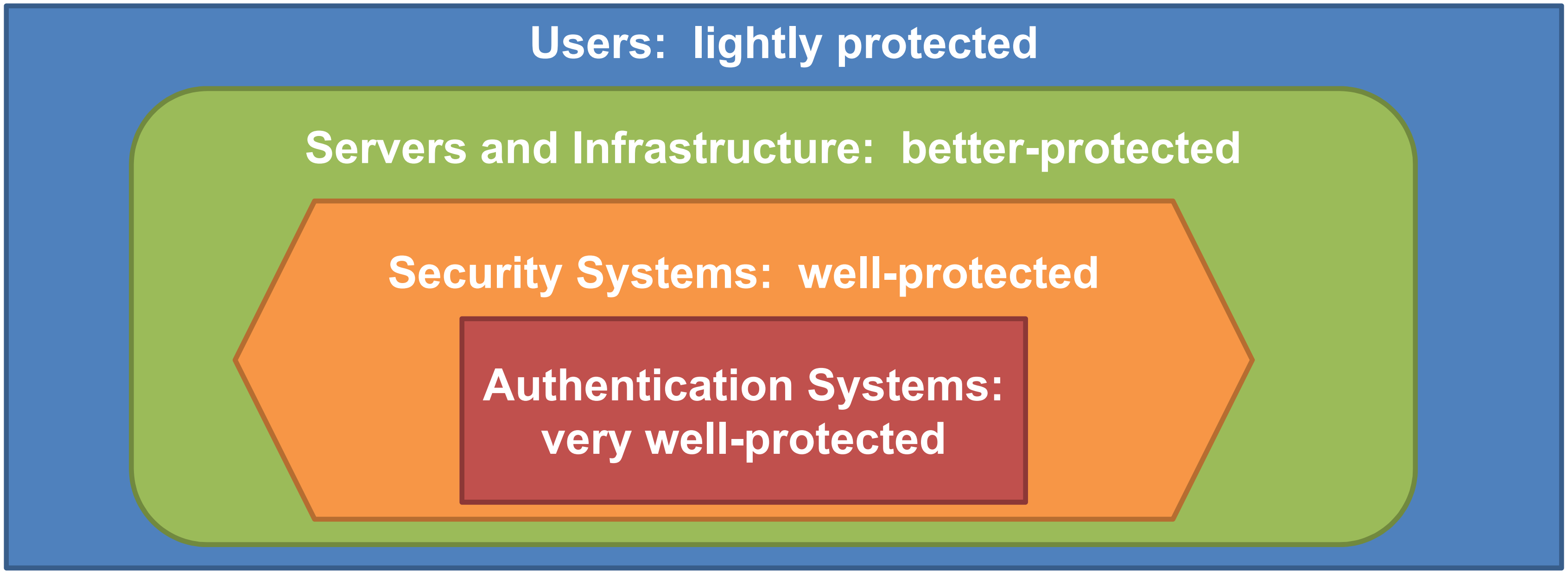
Town = Business Servers

Fields = Regular Users

Pragmatic Security: True Defense in Depth

Layer enterprise security to protect the security infrastructure best:

- Each layer gives defenders an opportunity to detect and repel attack
- Each layer’s defense can be somewhat porous – perfection not required
- Defenses get stronger as attackers penetrate further inside
- Goal is to give defenders 2 or more opportunities to catch the attack



Users: lightly protected

Servers and Infrastructure: better-protected

Security Systems: well-protected

Authentication Systems: very well-protected

Pragmatic Security: Top Ten

1. **Emphasis on detection** rather than protection
2. **Less reliance** on endpoint security
3. **Network segmentation** to provide defense in depth
4. **Two-factor authentication** for system administrators
5. **Application whitelisting** for critical systems and assets
6. **Log aggregation** and security information and event management (SIEM)
7. **24x7 security monitoring** to detect incidents
8. **Forensics tools** to track down attacks when they occur
9. **Incident rapid response** to repel attacks in real time
10. **Security incident metrics** tracking activities and threats

A Successful Cybersecurity Program

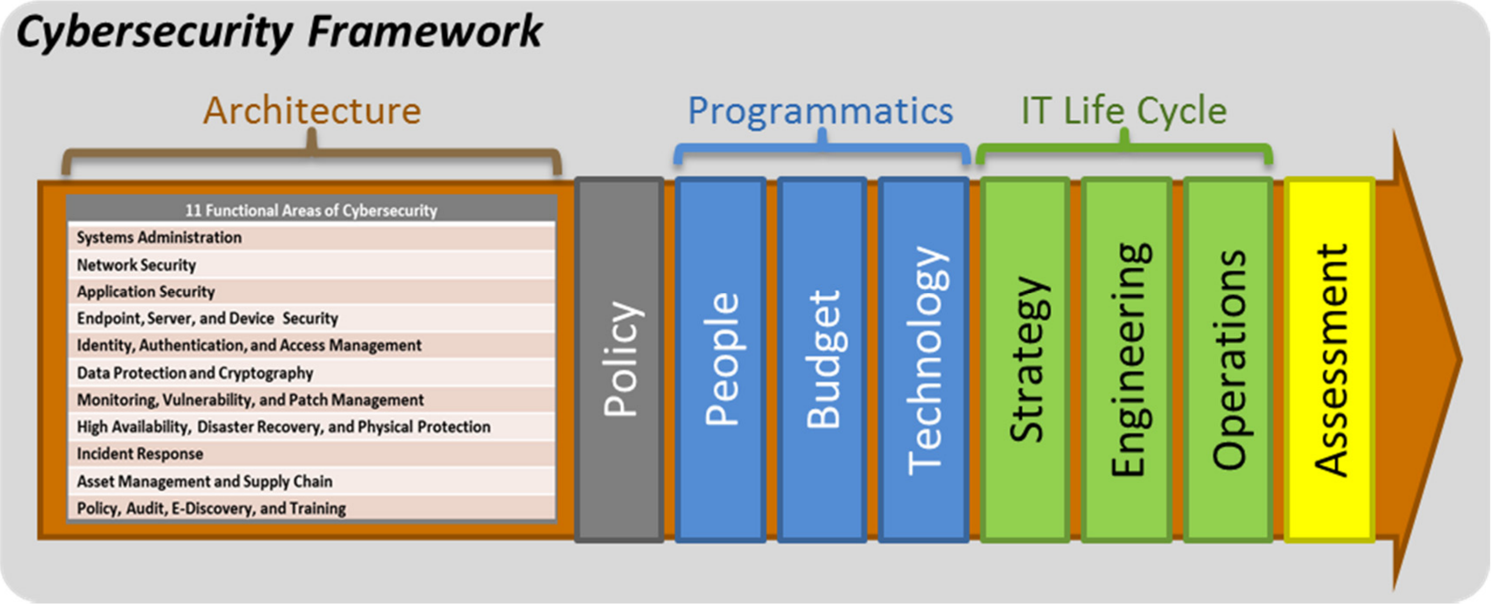
Characteristics

- More than just technologies
- Coordinate all of the following:
  - Cybersecurity Policy
  - Programmatics
  - IT life cycle
  - Assessment
- Combine to ***guide***, ***build*** and ***operate*** a successful program

Challenges

- ***Policy frameworks*** seldom align well with organization or assessment.
- ***Programmatic frameworks*** focus on business considerations, not cybersecurity
- ***IT life cycle frameworks*** do not support cybersecurity management or reporting
- ***Assessment frameworks*** do not tend to align with people organization or technology deployment

Elements of a Successful Program



Cybersecurity Framework

Architecture

11 Functional Areas of Cybersecurity
Systems Administration
Network Security
Application Security
Endpoint, Server, and Device Security
Identity, Authentication, and Access Management
Data Protection and Cryptography
Monitoring, Vulnerability, and Patch Management
High Availability, Disaster Recovery, and Physical Protection
Incident Response
Asset Management and Supply Chain
Policy, Audit, E-Discovery, and Training

Policy

Programmatics: People, Budget, Technology

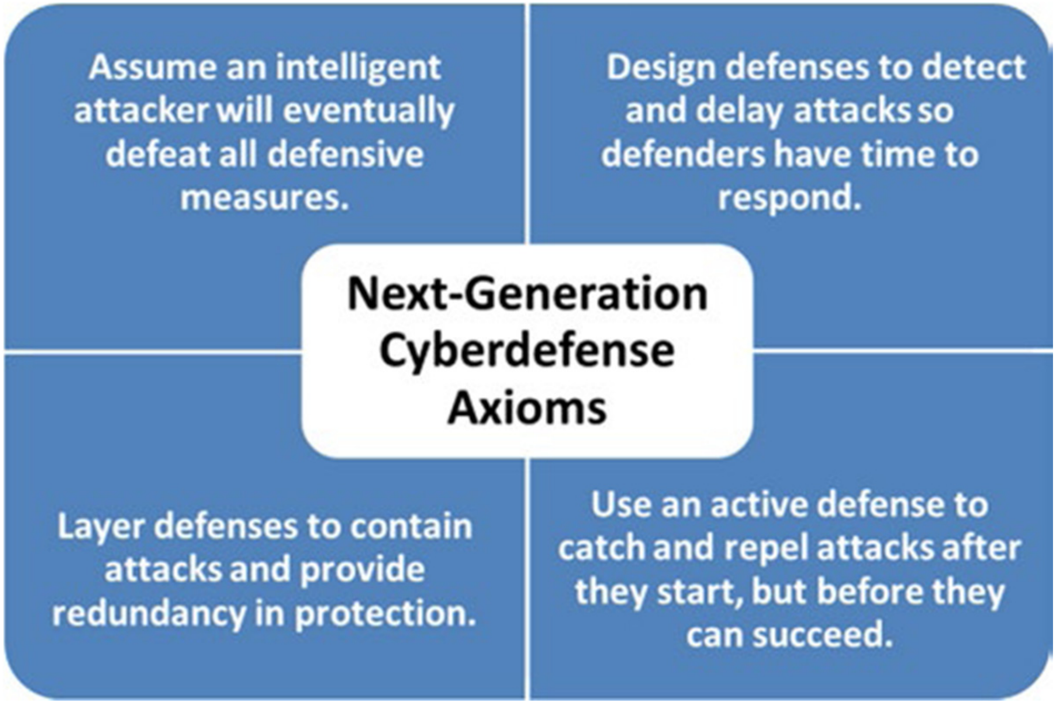
IT Life Cycle: Strategy, Engineering, Operations

Assessment

Requirements for a Successful Enterprise Cybersecurity Framework:

- Tie together **architecture**, **policy**, **programmatics**, **IT life cycle**, and **assessments** into a single framework
- Enables delegation of cybersecurity responsibilities into functional areas
- It needs to tie together **architecture**, **policy**, **programmatics**, **IT life cycle**, and **assessments** using a single framework for delegation and coordination
- Functional areas align well with real-world skills of cybersecurity professionals, and support budgets and technologies
- Functional areas enable easy delegation and reporting of status at an abstraction layer suitable for executive consumption
- Functional Areas support the business decision-making process for strategy and prioritization

Axioms for Cyberdefense



Assume an intelligent attacker will eventually defeat all defensive measures.

Design defenses to detect and delay attacks so defenders have time to respond.

Next-Generation Cyberdefense Axioms

Layer defenses to contain attacks and provide redundancy in protection.

Use an active defense to catch and repel attacks after they start, but before they can succeed.

Cybersecurity needs to be planned around the idea of achieving only partial security, rather than being resourced to do everything perfectly all the time.

Major cybersecurity frameworks lay out what the ***ideal*** practice should be, but have little, if any, guidance on how to deploy a ***partial*** solution that is the best value for the cost when the funding is not adequate to achieve the ideal.

Cybersecurity professionals must learn how to work with the business to find a balance between defenses that are only partially successfully, but effective in the eyes of the business.

Conclusion

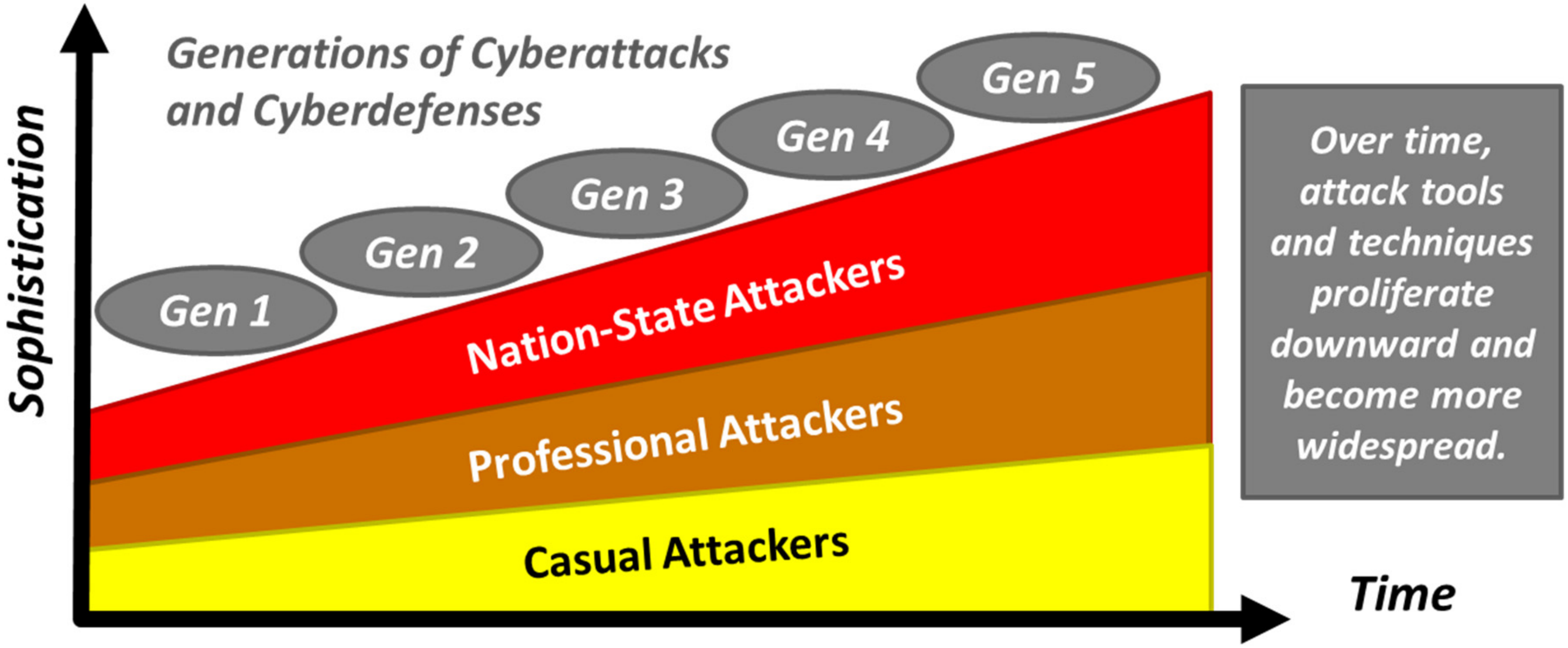
With a legacy cyber defense, the defender has to do everything perfectly to protect the enterprise.

With a next-generation cyber defense, the attacker has to do everything perfectly to attack it.

Which would you rather have?

6. Looking to the Future

- Cyberattacks and defenses can be characterized as generations.
- We are now in the transition from Generation 2 to Generation 3.
- There are more generations coming after this…



Over time, attack tools and techniques proliferate downward and become more widespread.