BITS Pilani

Pilani Campus

Cloud, IoT and Enterprise Security

Nishit Narang
WILPD-CSIS
(nishit.narang@pilani.bits-pilani.ac.in)

BITS Pilani

Pilani Campus

<SSCSZG570 , Cloud, IoT and Enterprise Security>

Lecture No. 3: Enterprise Security

Security as a Process + Securing Enterprise Network

Enterprise = Network + Systems + Data + Humans + …

Source Disclaimer: Content for many of the slides is from the course Textbook(s). Refer Course Handout for list of Textbooks.

Enterprise Security

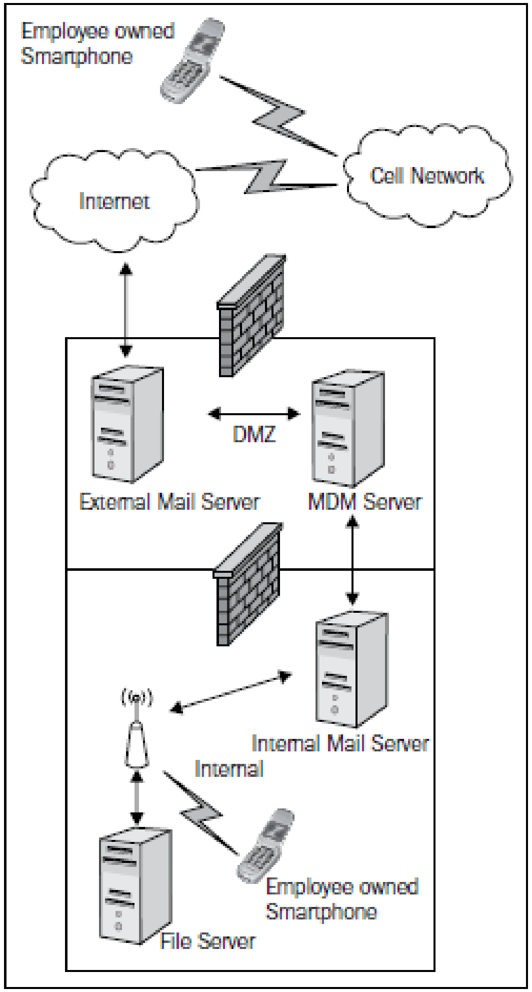
Modern Initiatives and Impacts to Security Architectures

BYOD Initiatives

- Bring your own laptop, cell, and tablet are a few of the new initiatives
  - This model is being used by many enterprises to reduce their IT budgets
- Enterprise Security Architecture aspects:
  - how to properly secure the device(s)
  - secure the network it connects to, and
  - secure the data that these devices will have access and data they shall possibly store
- Data access typically occurs through systems owned by the enterprise
- In next couple of slides, we will look at two of the common BYOD initiatives and discuss considerations when applying trust models to attempt securing the data accessed, transmitted, and stored on these consumer end points

BYOD: Mobile Devices

- Most mobile devices are cellular smartphones or tablets
  - Key use case is employee access to emails, calendar etc
- Commonly implemented security measures include using a Mobile Device Management (MDM) solution
  - Generic platform - determining what exact data the device has access to will be up to the enterprise to decide
  - The enterprise will have to map the interaction to a defined trust model or develop one to meet this request



Source: Aaron Woody, Enterprise Security: A Data-Centric Approach To Securing The Enterprise

BYOD: Personal Computers

Exploring the
ıre of Desktop Vi

- A more complicated initiative to secure, because maintaining a device by the enterprise that is not owned by the enterprise may cross some privacy and/or technical boundaries
  - However, there exist tremendous cost savings of allowing employees to bring their laptops to work to perform their jobs
- Some enterprises are leveraging virtualization in a "*trust no one*" model where the only way to access anything is through a virtual desktop environment
  - model is very secure, but comes at a cost to build a robust enough infrastructure to support it
- Other (generally smaller) organizations are allowing employees to bring their own PCs to access enterprise assets, with no virtualization and balancing access with risk
  - limit the access to all the data that has been assessed at a risk level of high and above, or to a level the enterprise's risk tolerance will allow

Security as a Process

Risk Analysis, Policies & Standards, Security Exceptions and Review of Changes

Overview

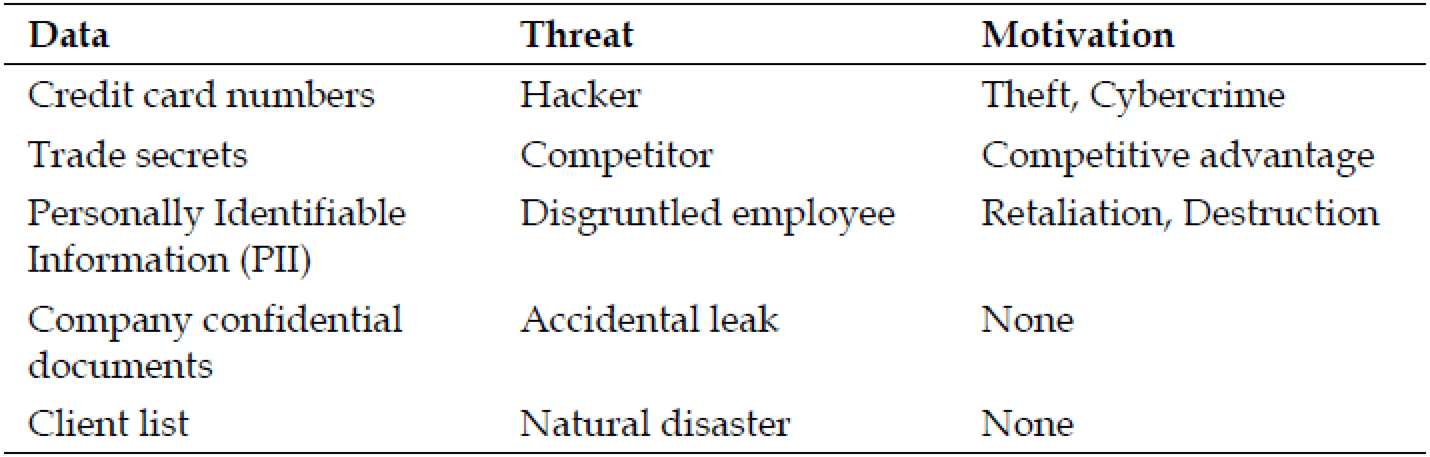
- Security is a process that requires the integration of security into business processes to ensure enterprise risk is minimized to an acceptable level
- We will introduce the concept of using risk analysis to drive security decisions, and to shape policies and standards for consistent and measurable implementation of security

Risk Analysis

- **Risk analysis** is the process of assessing the components of risk; threats, impact, and probability as it relates to an asset, in our case enterprise data
  - A simple risk analysis output may be the decision to spend capital to protect an asset based on value of the asset and the scope of impact if the risk is not mitigated
- It is the method to properly implement security architecture for enterprise initiatives
  - Without this capability, the enterprise will either spend on the products with the best marketing, or not spend at all
- In the next few slides, we take a closer look at the risk analysis components

Threat Assessment

- A **threat** is anything that can act negatively towards the enterprise assets
  - It may be a person, virus, malware, or a natural disaster
- Once a threat is defined, the attributes of threats must be identified and documented
  - The documentation of threats should include the type of threat, identified threat groupings, motivations if any, and methods of actions
- To gain understanding of pertinent threats for the enterprise, researching past events may be helpful
- Example:

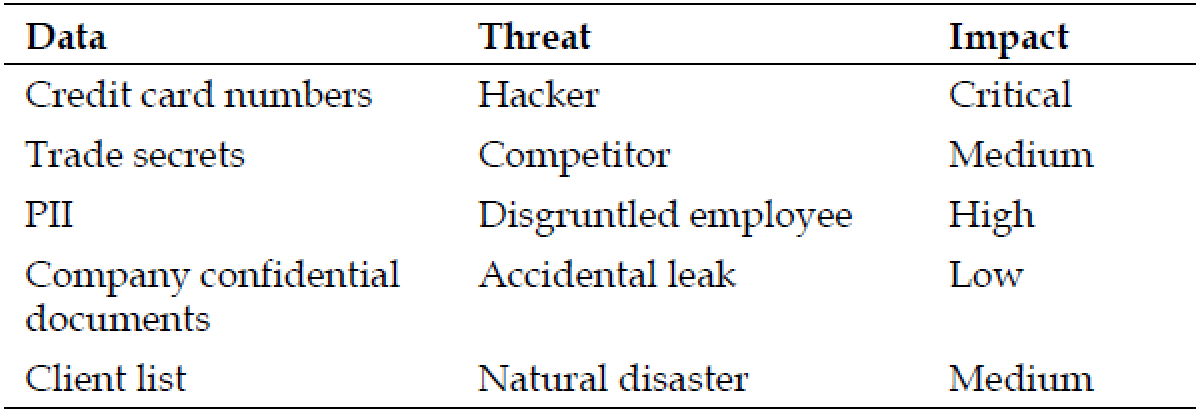


Data	Threat	Motivation
Credit card numbers	Hacker	Theft, Cybercrime
Trade secrets	Competitor	Competitive advantage
Personally Identifiable Information (PII)	Disgruntled employee	Retaliation, Destruction
Company confidential documents	Accidental leak	None
Client list	Natural disaster	None

Source: Aaron Woody, Enterprise Security: A Data-Centric Approach To Securing The Enterprise

Impact Assessment

- **Impact** is the outcome of threats acting against the enterprise. Examples:
  - a denial-of-service state where the agent, a hacker, uses a tool to starve the enterprise resources causing denial-of-service for legitimate users
  - the loss of customer credit cards resulting in online fraud, reputation loss, and countless dollars in cleanup and remediation efforts
- Types of Impacts: **Immediate** and **Residual**
  - Immediate impacts are rather easy to determine
  - Residual impacts are longer term and often known later
- Impact analysis needs to be thorough and complete. Example:

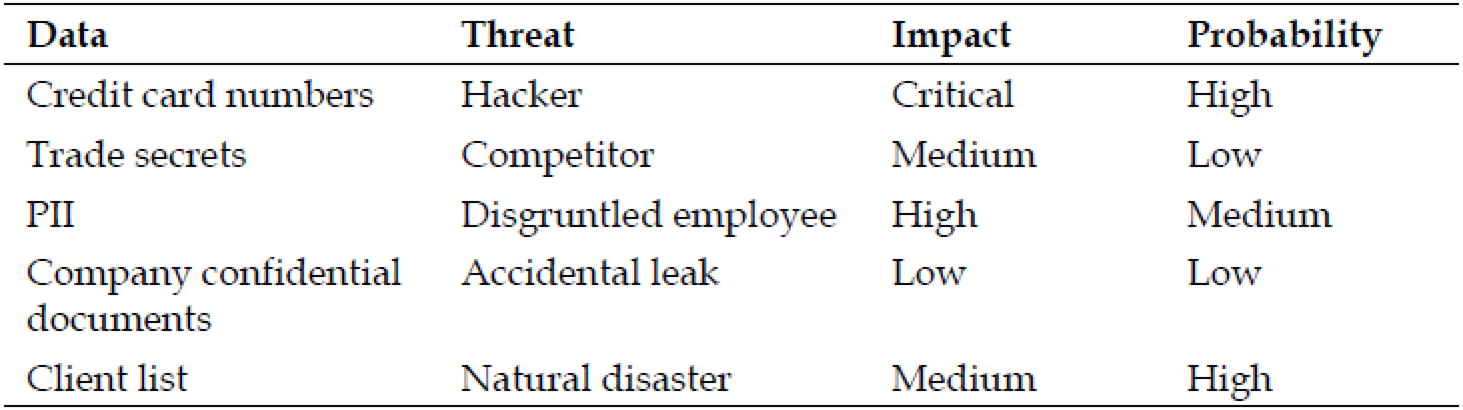


Data	Threat	Impact
Credit card numbers	Hacker	Critical
Trade secrets	Competitor	Medium
PII	Disgruntled employee	High
Company confidential documents	Accidental leak	Low
Client list	Natural disaster	Medium

Source: Aaron Woody, Enterprise Security: A Data-Centric Approach To Securing The Enterprise

Probability Assessment

- **Probability** is the likelihood of the Risk to mature
  - if threat actions may only occur once in three thousand years, investment in protecting against the threat may not be warranted
- Probability data is as difficult, if not more difficult, to find than threat data
- Probability and Impact are equally important to decide whether (or not) to handle a threat. It is the combination, normally, that matters
  - Example, in the game of Russian roulette, a semi-automatic pistol either has a bullet in the chamber or it does not. With a revolver and a quick spin of the cylinder, you now have a 1 in 6 chance on whether there is a bullet that will be fired when the firing pin strikes. How do you assess the Risk?



Data	Threat	Impact	Probability
Credit card numbers	Hacker	Critical	High
Trade secrets	Competitor	Medium	Low
PII	Disgruntled employee	High	Medium
Company confidential documents	Accidental leak	Low	Low
Client list	Natural disaster	Medium	High

Source: Aaron Woody, Enterprise Security: A Data-Centric Approach To Securing The Enterprise

Assessing Risk

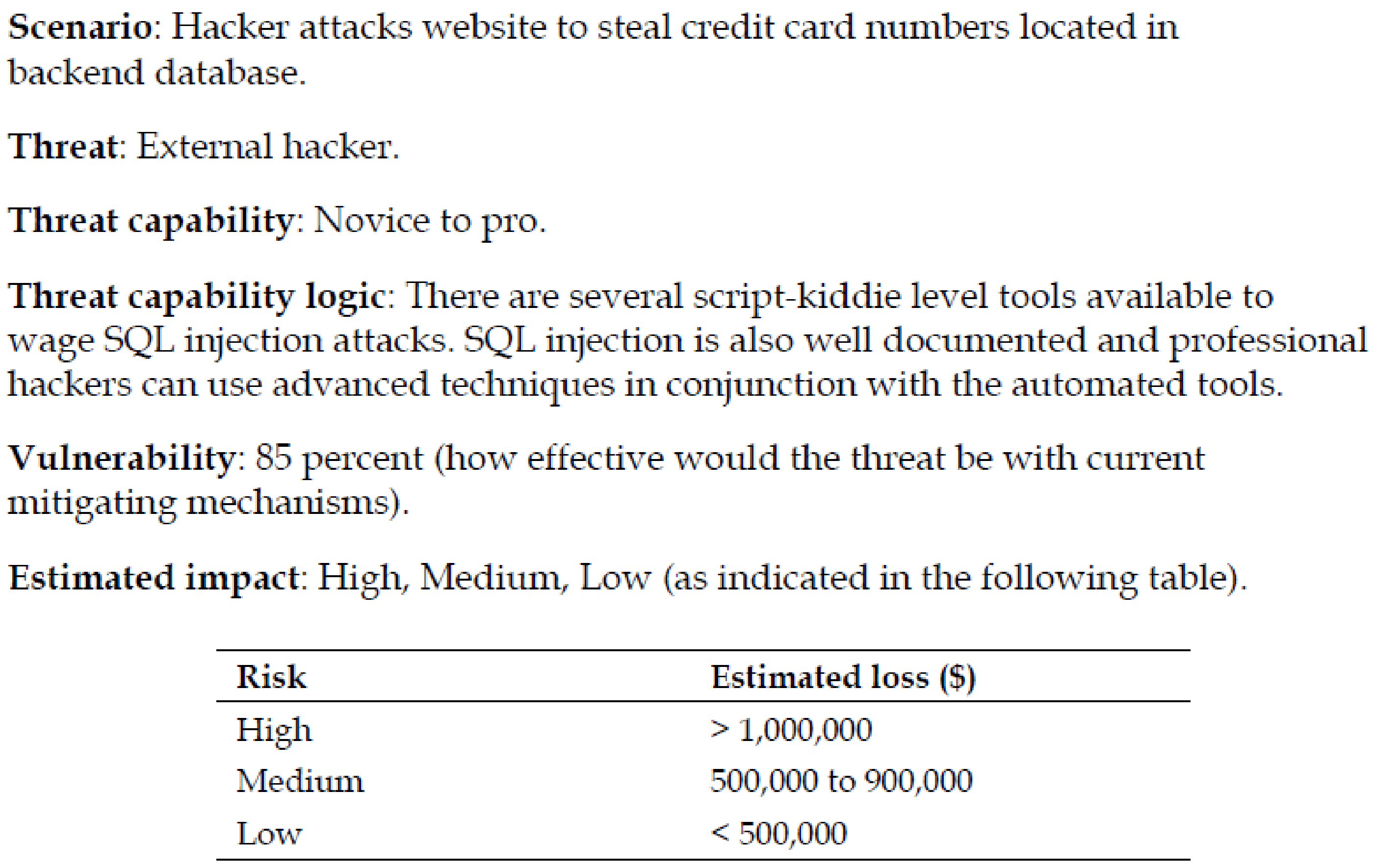
- Now that we have identified threats to the data, rated the impact to the enterprise, and estimated the probability of the impact occurring, the next logical step is to calculate the risk of the scenarios
- There are two methods to analyze and present risk: **qualitative** and **quantitative**
  - The decision to use one over the other should be based on the maturity of the enterprise's risk office/ team
  - In general, a quantitative risk analysis will use descriptive labels like in any qualitative method
  - However, there is more financial and mathematical basis involved in a quantitative analysis

Qualitative Risk Analysis

- Qualitative risk analysis provides a perspective of risk in levels with labels such as Critical, High, Medium, and Low
  - The enterprise must still define what each level means in a general financial perspective
  - For instance, a Low risk level may equate to a monetary loss of $1,000 to $100,000
  - The dollar ranges associated with each risk level will vary by enterprise

Qualitative Risk Analysis

- Example Exercise:



Scenario: Hacker attacks website to steal credit card numbers located in backend database.

Threat: External hacker.

Threat capability: Novice to pro.

Threat capability logic: There are several script-kiddie level tools available to wage SQL injection attacks. SQL injection is also well documented and professional hackers can use advanced techniques in conjunction with the automated tools.

Vulnerability: 85 percent (how effective would the threat be with current mitigating mechanisms).

Estimated impact: High, Medium, Low (as indicated in the following table).

Risk	Estimated loss ($)
High	> 1,000,000
Medium	500,000 to 900,000
Low	< 500,000

Source: Aaron Woody, Enterprise Security: A Data-Centric Approach To Securing The Enterprise

Quantitative Risk Analysis

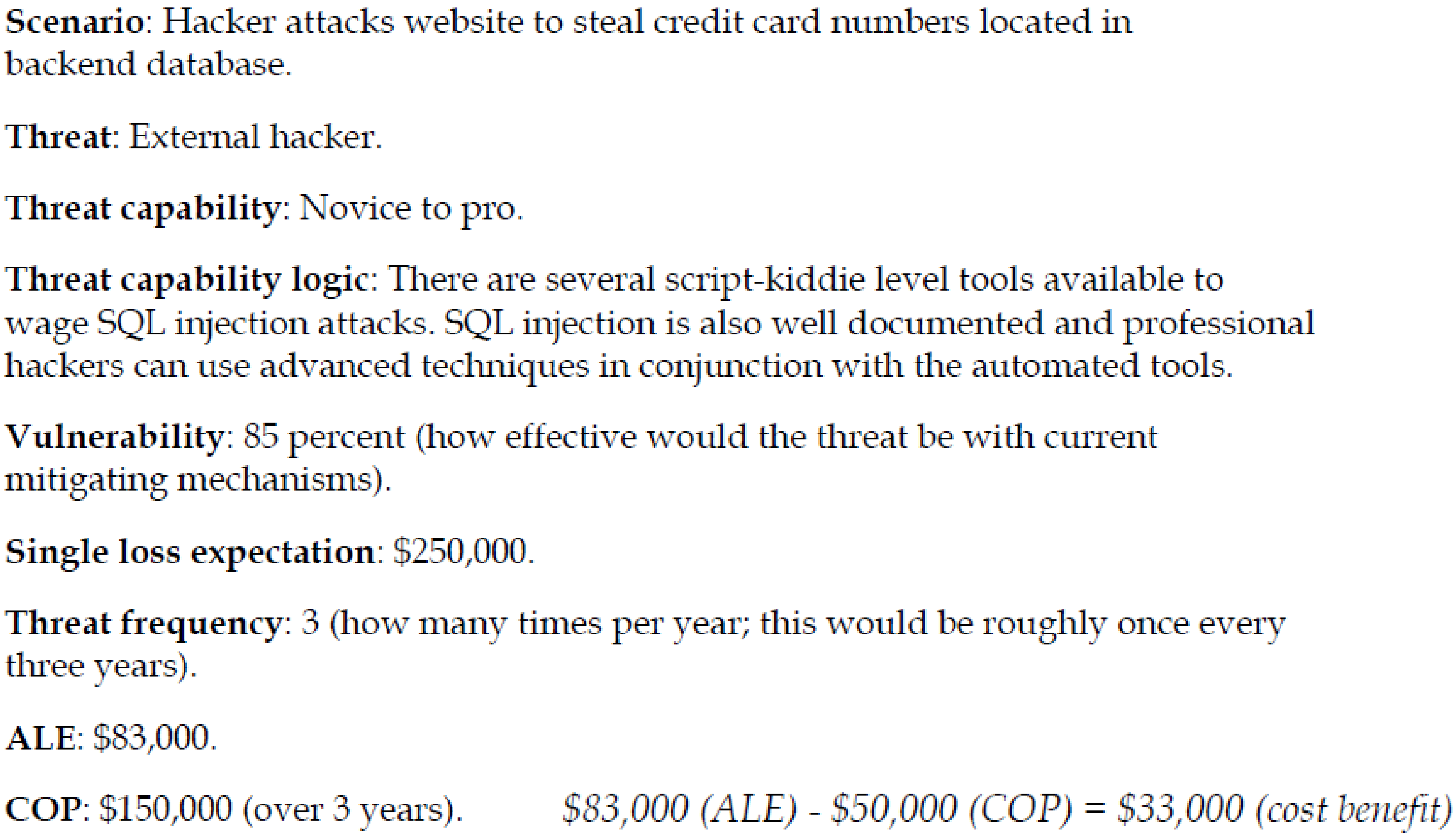
- Quantitative risk analysis is an in-depth assessment of what the monetary loss would be to the enterprise if the identified risk were realized
  - In order to facilitate this analysis, the enterprise must have a good understanding of its processes to determine a relatively accurate dollar amount for items such as systems, data restoration services, and man-hour break down for recovery or remediation of an impacting event
  - Enterprises with a mature risk office will undertake this type of analysis to drive priority budget items or find areas to increase insurance, effectively transferring business risk
  - Ideally, the cost to mitigate would be less than the loss expectancy over a determined period of time. This is simple return on investment (ROI) calculation

Quantitative Risk Analysis

- A Few Definitions:
  - **Annual loss expectancy** (**ALE**): The ALE is the calculation of what the financial loss would be to the enterprise if the threat event was to occur for a single year period
    - This is directly related to threat frequency
    - In a scenario, if this is once every three years, dividing the single lost expectancy by annual occurrence provides the ALE
  - **Cost of protection** (**COP**): The COP is the capital expense associated with the purchase or implementation of a security mechanism to mitigate or reduce the risk scenario
    - An example would be a firewall that costs $150,000. For a 3-year loss expectancy period, this is $50,000 per each year of protection
    - If the cost of protection (over the same period) is lower than the loss, it is a good indication the investment is financially worthwhile

Quantitative Risk Analysis

- Example Exercise:



Scenario: Hacker attacks website to steal credit card numbers located in backend database.

Threat: External hacker.

Threat capability: Novice to pro.

Threat capability logic: There are several script-kiddie level tools available to wage SQL injection attacks. SQL injection is also well documented and professional hackers can use advanced techniques in conjunction with the automated tools.

Vulnerability: 85 percent (how effective would the threat be with current mitigating mechanisms).

Single loss expectation: $250,000.

Threat frequency: 3 (how many times per year; this would be roughly once every three years).

ALE: $83,000.

COP: $150,000 (over 3 years). *$83,000 (ALE) - $50,000 (COP) = $33,000 (cost benefit)*

Source: Aaron Woody, Enterprise Security: A Data-Centric Approach To Securing The Enterprise

Security Policies and Standards

- Policy versus standard
  - Policy dictates what must be done, whereas Standard states how it gets done
  - A policy's intent is to address behaviors and state principles for IT interaction with the enterprise
  - Standards focus on configuration and implementation based on what is outlined in policy
- Example:
  - An employee cell phone policy may be created in response to the business request to use personal phones for business
  - However, with the ability to use a personal cell phone, there may be restrictions on using the "smart" features to access enterprise data, or a requirement to load a mobile device management application on the cell phone
  - The standard in this scenario may be a requirement of a certain smart phone operating system type and version level. This may be driven by management and security capabilities of the platform
- Role of Tools
  - Tools need to be implemented to measure compliance and provide enforcement of policies and standards

Security Policy Development

- Driven typically by an outside driver such as regulatory compliance, industry certification, or business driver
  - regulatory compliance, example, **Payment Card Industry Data Security Standard** or **PCI DSS**
- Typical set of security policies includes:
  - Information security policy
  - Acceptable use policy
  - Technology use policy
  - Remote access policy
  - Data classification policy
  - Data handling policy
  - Data retention policy
  - Data destruction policy

Information Security Policy

- General policy that addresses all the security-specific requirements that may or may not be addressed in other policies
  - outline of what is expected from employees to ensure technology implementations and use are on par with enterprise security posture
    - Example, use of only secure protocols, logging requirements of systems, requirement for regular risk analysis etc
  - policy in effect makes known that IT security exists
    - provides the basis for the security team to protect the enterprise data. This includes giving the right to monitor employee use of systems and data access and install software to do so
- What can be a starting point for a new organization?
  - SANS Security Policy Project has templates that can serve as a base or be used as is with little modification
  - https://www.sans.org/information-security-policy/

Acceptable Use Policy

- A ***code of conduct***, with consequences described for failure to comply!
  - may include items such as the network, employer provided equipment, website access, e-mail, and other use-based technologies
- Focus of this policy is to reduce not only security risk to the enterprise but legal liability too
  - example policy statement: "*employer-provided equipment must be used only for employer-sanctioned activities*"
  - What services are employees permitted to use?
  - What services can be abused and introduce risk?
  - What is the consequence for violating the policy?

Technology Use Policy

- May be developed separately from the acceptable use policy to call out specific technologies allowed and their approved use
  - Example, could be used to capture items such as BYOD initiatives or cloud initiatives
  - What is the technology?
  - How can it be used for better productivity?
  - What types of data can the technology access?
  - Who will be permitted to use the technology?
  - How will data and network access via the technology be managed?
  - ……

Remote Access Policy

- Defines what types of devices and who may connect to the enterprise network remotely
- Includes the appropriate authentication methods such as two-factor or simple username and password
- Some enterprises are very strict on employer-owned devices being the only method to use a VPN connection to the employer network

Data Classification Policy

- In a data-centric model for security architecture, data classification is an absolute
  - must know what data exists, where it resides, and how to protect it
  - data should be mapped to a classification model that outlines its sensitivity and high-level protection requirements
- Anytime new data is generated or old data discovered, it should go through the process of classification
  - Typically, data types will follow standard enterprise data labeling such as, confidential, restricted, and public
  - Based on the labeling, data protection scheme can be defined (e.g. Encryption, Restricted Access, or No Protection)

Data Handling Policy

- This policy is prescriptive on approved interactions with enterprise data
  - Interactions may be people, applications, or automation
  - A closely integrated policy would be the data classification policy
- Includes:
  - Acceptable storage for enterprise data
  - Enforcement of secure handling of appropriately classified data
  - Access and authorization procedures for sensitive data

Data Retention Policy

- A data retention policy simply states the length of time to retain data in the enterprise
  - The general rule is to only keep data as long as needed for data recovery and regulatory requirements
  - Maintaining data for long periods of time significantly increases the risk of data leakage
  - possible damage to the enterprise can be reduced by enforcing data retention limits
- This policy is tightly related to the data destruction policy

Data Destruction Policy

- A data destruction policy provides an enforceable and measurable method to ensure data is properly destroyed
  - Example: sanitize hard drives before trashing them
- Includes:
  - Requirement to securely wipe all functioning hard disks
  - Requirement to physically destroy non-working hard disks, tapes, and so on
  - If completed by third party, a formal process developed with verification
  - Labeling of systems with data that require destruction
  - Clear consequences for negligent data leakage

Enterprise Security Standards

- Wireless Network Security Standard
  - wireless networking extends the network outside of the physical bounds of the brick-and-mortar enterprise
  - The following are a few examples of wireless network security standards:
    - Implementation of WPA2-Enterprise
    - Two-factor authentication using certificates
- Enterprise Monitoring Standard
  - security monitoring of systems, networks, and users
  - necessary for both policy enforcement and as an implemented security mechanism
  - standard list of audit trail information

Enterprise Security Standards

- Enterprise Encryption Standard
  - Data encryption required for data in transit, storage, or being processed
  - The following are the areas to focus on to standardize encryption :
    - Whole disk encryption
    - Database encryption
    - File-level encryption
    - Secure transport encryption
  - Key management is probably the most involved and difficult task with encryption
- System Hardening Standard
  - reducing the attack surface of a system by
    - turning off unnecessary services,
    - patching the operating system and software, and
    - enabling attack mitigation features such as iptables for Linux and Windows Firewall for Windows
  - following are a few hardening guide sources:
    - NIST (http://csrc.nist.gov/groups/SNS/checklists/)
    - NSA (http://www.nsa.gov/ia/mitigation_guidance/security_ configuration_guides/operating_systems.shtml)
    - Microsoft (http://www.microsoft.com/en-us/download/details.aspx?id=16776)

innovate achieve lead

BITS Pilani

Pilani Campus

Securing the Enterprise Network

What we will cover?

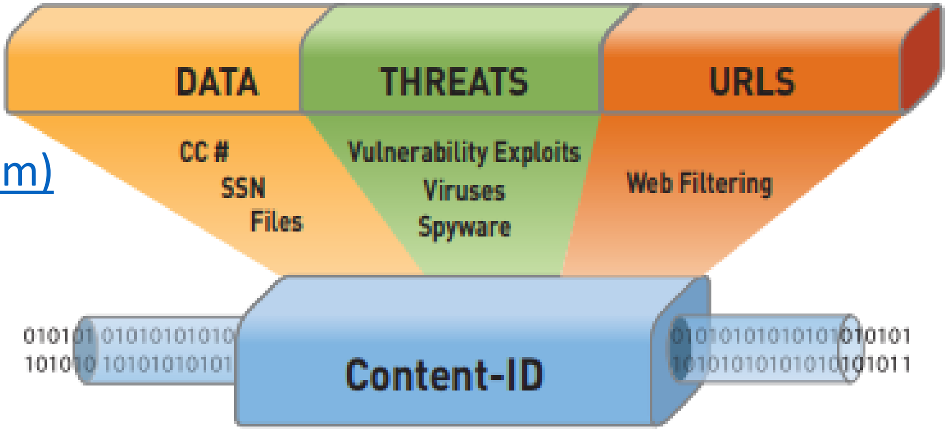
- Notion of ***Defence-in-Depth***
  - Securing each tier of the enterprise network to mitigate attacks against assets at each tier
- Introduce multiple technologies that can be implemented in the network
  - secure enterprise infrastructure, network services such as e-mail, DNS, file transfer, and web applications
- Advancement in firewall technologies
  - provide more in-depth inspection and protection capabilities
- Intrusion detection and prevention
  - protect against simple and the most advanced attacks across applications, systems, and network services
- Security through network segmentation

Defence In Depth

- When developing an enterprise security strategy, a layered approach is the best method to ensure detection and mitigation of attacks at each tier of the network infrastructure
  - *"Defence in depth is a* ***military strategy*** *that seeks to delay rather than prevent the advance of an attacker, buying time and causing additional casualties by yielding space. Rather than defeating an attacker with a single, strong defensive line, defence in depth relies on the tendency of an attack to lose momentum over time or as it covers a larger area."* Source: Wikipedia
- Although the enterprise network perimeter is changing, the basic network security mechanisms still have their purpose
  - the same types of security mechanisms need to persist, however, where they are implemented may change slightly depending upon the network architecture
- In general, we will not focus much on where the network perimeter is, but on what needs to be protected

Next Generation Firewalls

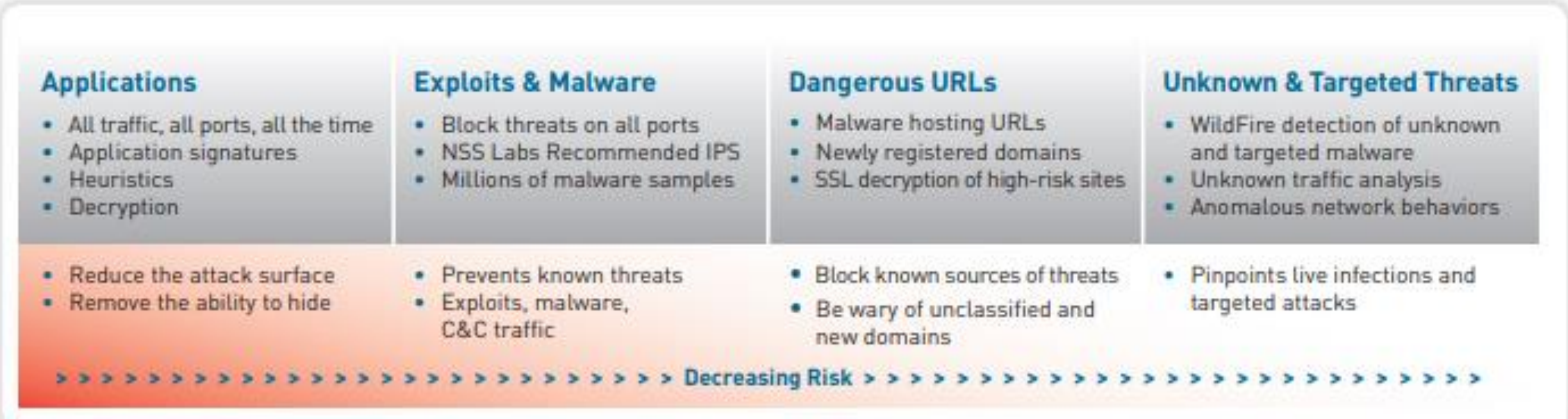
- Standard firewalls simply check for the policy allowing the source IP, destination IP, and TCP/UDP port, without a further deep packet analysis
- Next Generation Firewalls (NGFW) perform more deep packet analysis to mitigate malicious traffic masquerading as legitimate
  - Example: DNS traffic inspected by a standard firewall may look legitimate, but in reality, the DNS packets may be padded with data that is being ex-filtrated from the network
- An NGFW can inspect traffic for data, threats, and web traffic



Content_ID_tech.pdf (paloaltonetworks.com)

Palo Alto
etworks - ContentI

Case Study: Content-ID

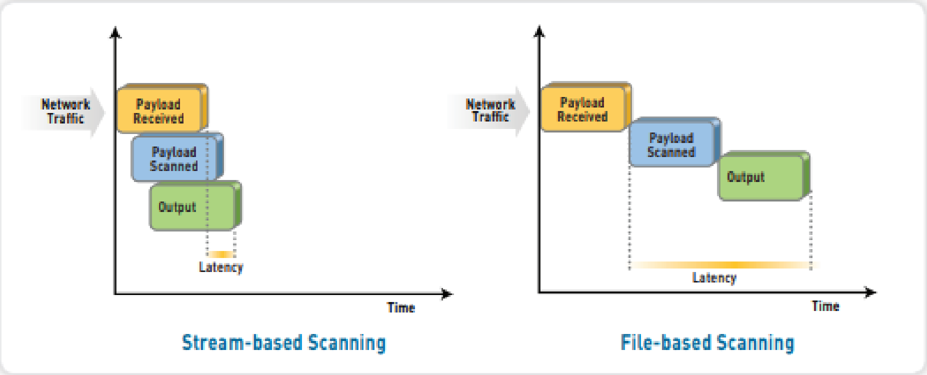


Applications	Exploits & Malware	Dangerous URLs	Unknown & Targeted Threats
• All traffic, all ports, all the time • Application signatures • Heuristics • Decryption	• Block threats on all ports • NSS Labs Recommended IPS • Millions of malware samples	• Malware hosting URLs • Newly registered domains • SSL decryption of high-risk sites	• WildFire detection of unknown and targeted malware • Unknown traffic analysis • Anomalous network behaviors
• Reduce the attack surface • Remove the ability to hide	• Prevents known threats • Exploits, malware, C&C traffic	• Block known sources of threats • Be wary of unclassified and new domains	• Pinpoints live infections and targeted attacks

> Decreasing Risk >

Source: PALO ALTO NETWORKS

- Single-pass architecture (SP3) integrates multiple threat prevention disciplines (IPS, anti-malware, URL filtering, etc) into a single stream-based engine with a uniform signature format
- Allows traffic to be fully analyzed in a single pass without the incremental performance degradation seen in other multi-function gateways



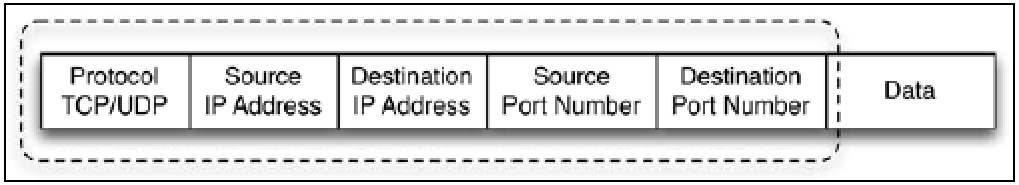
Stream-based scanning
Stream-based scanning helps minimize latency and maximize throughput performance.

NGFW: Benefits and Challenges

- **+** Most significant benefit of the NGFW is **awareness** due to deep-packet inspection and analysis
- **+** Reduced DMZ complexity - with next generation firewalls, new technologies become a part of the firewall tier, including intrusion prevention, user authorization, application awareness, and advanced malware mitigation
- **-** This shift in firewall capabilities may add confusion to the role the appliance plays in the overall network protection
- **-** In comparison to web application and database firewalls, while the next generation firewall provides some coverage across these areas today, the available platforms do not have the advanced capabilities of purposefully designed web application firewalls or database firewalls
  - NGFW is capable of basic detection and mitigation of common web application attacks, but lacks the more in-depth coverage provided by web application firewalls with database counterparts
  - Thus, implementing a NGFW in addition to web application and database firewalls provides the most comprehensive coverage for a network

NGFW: Application Awareness

- Traditional firewalls only look at the source and destination IP addresses and the TCP or UDP port to make a decision to block or permit a packet



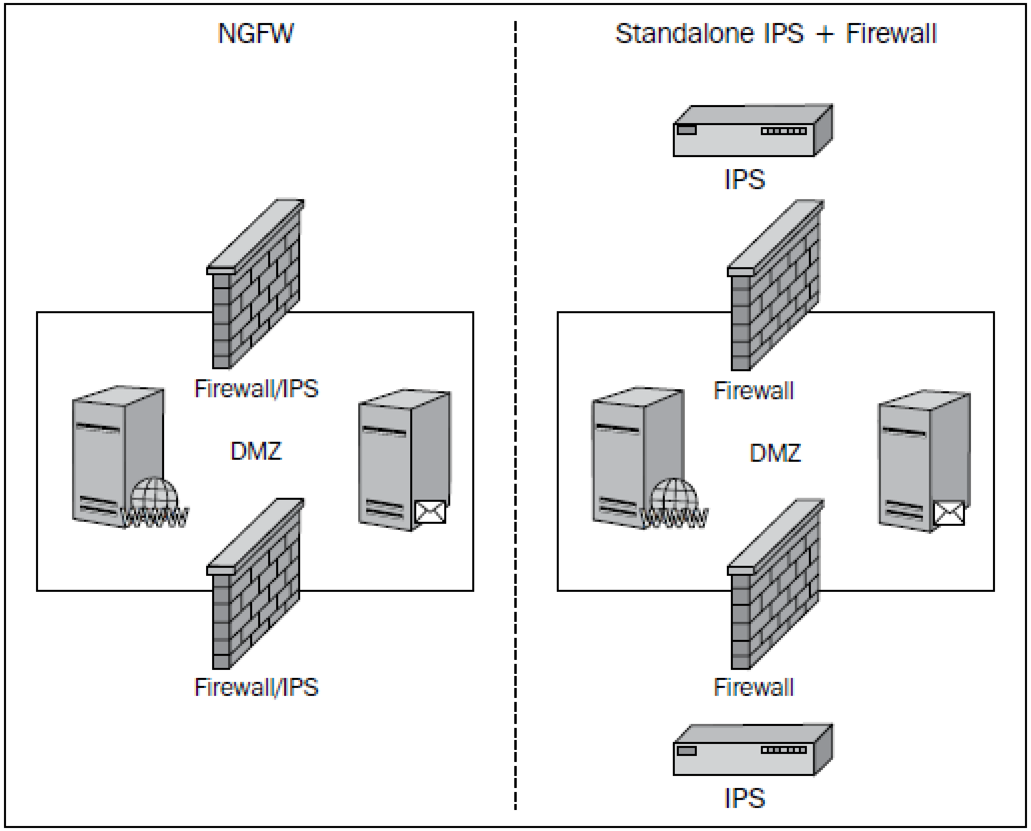
Protocol TCP/UDP	Source IP Address	Destination IP Address	Source Port Number	Destination Port Number	Data

Simplified TCP packet with IP header with header inspection only

- NGFW is able to perform deep packet inspection to also decode and inspect the application data in network communication
  - Some firewall manufacturers, such as Palo Alto Networks, are able to identify over 3000 unique applications as traffic traverses the firewall
  - Offers ability to identify and take action on network traffic that violates security policy – e.g. torrent clients, anonymous proxy services, and tunneled connections back to a home, office, or other unapproved destinations

NGFW: Intrusion Prevention

- Intrusion prevention coverage is normally required for every connection to the enterprise network
  - With the average cost of an IPS being over $40,000, this adds up quickly in addition to the support and maintenance costs
  - Simplifies management of IT security and the skillsets required to operationally support the solution
  - One less appliance in the DMZ - increases the performance



Source: Aaron Woody, Enterprise Security: A Data-Centric Approach To Securing The Enterprise

NGFW: Malware mitigation

- The newest addition to the features that NGFWs are offering is advanced malware protection in the form of botnet identification along with malware analysis in the cloud
  - Performed by a solution built into the firewall, where the malware is examined in the cloud, protection developed and mitigation implemented by the manufacturer
- While the next generation firewall implementation is less mature than the standalone solutions, leveraging the cloud and the vendor's entire customer base to provide samples will increase the effectiveness and value of the feature

IDS/IPS

- Intrusion detection and prevention technology has remained a mainstay at the network perimeter
  - While several firewall technologies are integrating intrusion prevention into their offerings, there has not been a complete shift to this implementation
- Intrusion detection is a method for detecting an attack but taking no action
  - this has been abandoned at the network perimeter when a breach is undesirable
  - it seems to still have a significant implementation in the internal network server segments to passively observe the behaviors of internal network users
  - has all the detection logic of intrusion prevention but without the ability to actively mitigate a threat
- Intrusion prevention is similar to intrusion detection, but has the capability to disrupt and mitigate malicious traffic by blocking and other methods
  - Many IPS devices have purposefully built denial of service mitigation technology
  - can be deployed at the network perimeter
  - should also be considered for implementation in the internal network to protect the most critical assets within the organization
- As the attacks have become advanced, there is debate on the overall advantage of the IDS/IPS
  - However, a defense in-depth strategy is best implemented by including IDS/IPS as an essential network protection mechanism

IDS/IPS: Detection Methods

- IDS/IPS devices use a combination of three methods to detect and mitigate attacks
  - behavior, anomaly, and signature
  - initial IDS/IPS systems were specialized in one method or another
  - Today, it is rare to find a detection method without the others
  - Also because attacks are not always as simple as protocol misuse or a known Trojan signature