CYBER503x
Cybersecurity Risk Management

Unit 5: Security Metrics

“To Measure is To Know”

- Security is a process; process is routine, institutional and operational; process is measureable.
- Sample business metrics:
  - “cost per square”, “inventory turns” in supply chain industry
  - “website conversion rate”, “subscription cost to acquire” in e-commerce
- Key characteristics of metrics:
  - Incorporate measures of time or money
  - Are well understood across the company
  - Are well understood across industries and are consistently measured
  - Are calculated mechanically

Analogous Examples

- Information security is one of the few areas of management that does not posses a well-understood canon of techniques for measurement.
  - In finance, “value-at-risk” techniques
  - Quality assurance literature (measure quality)
  - Public health and disease control (get the “big picture”)
  - Portfolio management (balance risk and reward)
  - Accelerated failure testing (similar to penetration test)
  - Insurance (evolving data, moving windows)
- Knowing what to measure, how to measure it and how to communicate those metrics can help improve security’s efficiency, effectiveness and standing in the business world.

“Metrics” Defined

- A Metric is “a consistent system or standard of measurement”.
- IT Metrics:
  - Value delivery (doing the right thing)
  - Process improvement (doing things right)
- The primary goal of metrics is to quantify data to facilitate insight.
  - Helping diagnose a particular subject area or understand its performance
  - Quantifying particular characteristics of the chosen subject area
  - Facilitating “before-and-after”, “what-if”, “why/why-not” inquire
  - Focusing discussion about the metrics themselves on causes, means and outcome rather than on methodologies used to derive them.

What's Wrong with ALE=SLE x AOR?

- Annual Loss Expectancy is a popular paradigm in the information security
  - Models the impact that security events have on assets.
  - ALE is a relatively easy and simple algebraic formula that multiplies the value of a discrete loss event (SLE) by its expected annual occurrence.
- ALE problems: "lots of guess work"
  - The inherent difficulty in modeling outliers.
    - "Security events are low frequency and high severity". Outliers dominate loss events. Hard to characterize a "typical" loss event.
    - ALE model encourages practitioners to think about dollar impact on an aggregate, averaged basis, in spite of the fact that losses do not navigate to the middle; they cluster on the far edges.
  - The lack of data for estimating probabilities of occurrence or loss expectancies.
  - Sensitivity of the ALE model to small changes in assumptions.
    - ALE model contains only a few variable.

Why Security Metrics?

- Security is not a product, it is a process.
  - *"Is my security better this year?"*
  - *"What am I getting for my security dollars?"*
  - *"How do I compare with my peers?"*
- ISO 17799 acknowledges: "a comprehensive and balanced system of measurement which is used to evaluate performance in information security management" is a critical success factor for information security.
- Challenges:
  - Unwillingness to share security information
  - Lack of common definitions for terms and metrics
  - Legal concerns and incentive failures are also roadblocks to data sharing
  - More regulation vs. more measurement?

Security Metrics:
The purpose and benefits

- Key security questions for business leaders:
  - *How effective are my security processes?*
  - *Am I better off than I was this time last year?*
  - *How do I compare with my peers?*
  - *Am I spending the right amount of money?*
  - *What are my risk transfer options?*
- Benefits:
  - Understand security risks
  - Spot emerging problem
  - Understand weaknesses in their security infrastructure
  - Measure performance of countermeasure process
  - Recommend technology and process improvement

Security Metrics

- Secure metrics are the measurements to support the decisions regards security risk management:
  - Measure the likelihood and the potential consequences of an identified risk
  - Measure how effective the security operations are
  - Measure to understand the risk environment
- Security metrics must be about ROSI: Return on Security Investment

Types of Security Metrics

- Technical security metrics
  - Used to diagnose problems and measure technical security activities)
- Security Program metrics
  - Used to measure overall program effectiveness, such as risk management, policies compliance, employee training, identity management, etc.
- Security scorecard
  - Uses above two sets of metrics to build a balanced security scorecard.

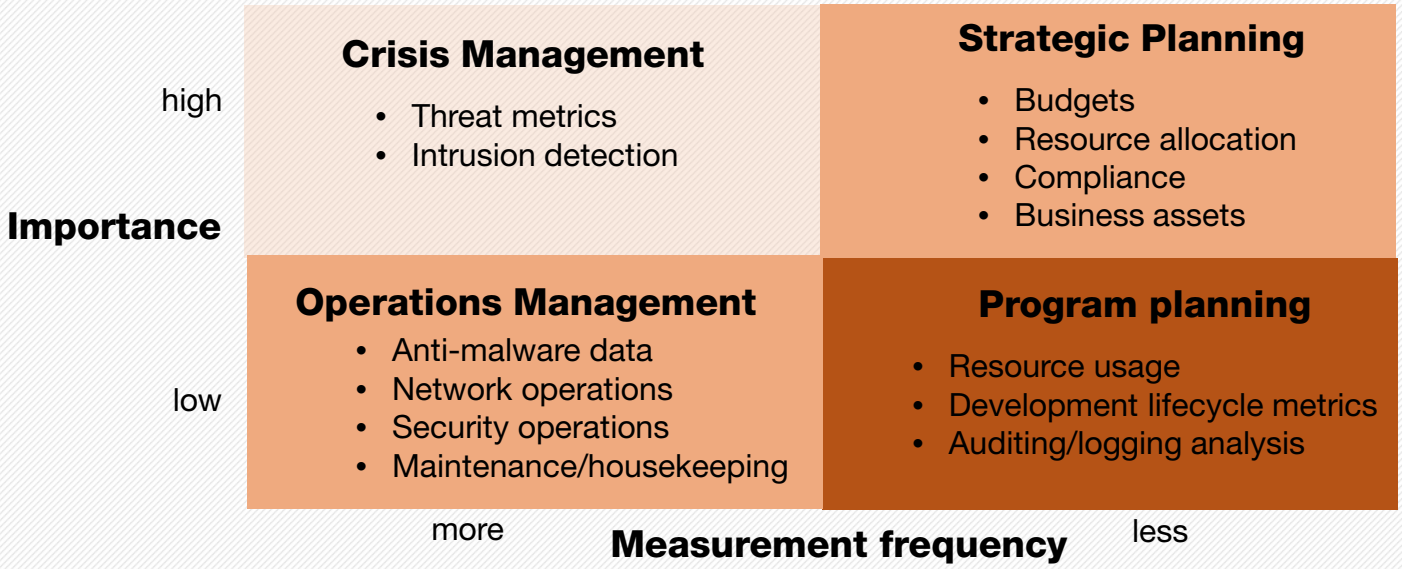
A comprehensive and balanced system of measurement which is used to evaluate performance in information security management is a critical success factor for information security.

Modelers vs. Measurers

- Security Modeling: threat, risk and losses.
  - Top Down approach
  - Scientific theorists
- Security Measurements: metrics, metrics, metrics
  - Bottom Up approach
  - Experimentalists

Good Metrics (1)

- Consistently measured, without subjective criteria
  - Metrics vs. Ratings
- Cheap to gather (in terms of time and money), preferably in an automated way with a short sampling intervals.



Good Metrics (2)

- Expressed as a cardinal number of percentage, not with qualitative labels like “high”, “medium” and “low”
- Expressed using at least one unit of measure, such as “defects”, “hours”, or “dollars. (for benchmarking)
  - Two units of measure are better, e.g. “number of application security defects per 1000 lines of code”
- Metrics with short sampling intervals help companies analyze their security effectiveness on a day-to-day and week-to-week basis rather than through a yearly rearview mirror.
- Contextually specific, relevant enough to decision-makers so that they can take actions.
  - “average number of attacks” vs. scoping the same metric down to business units (to make specific decisions about security provisioning and staffing)

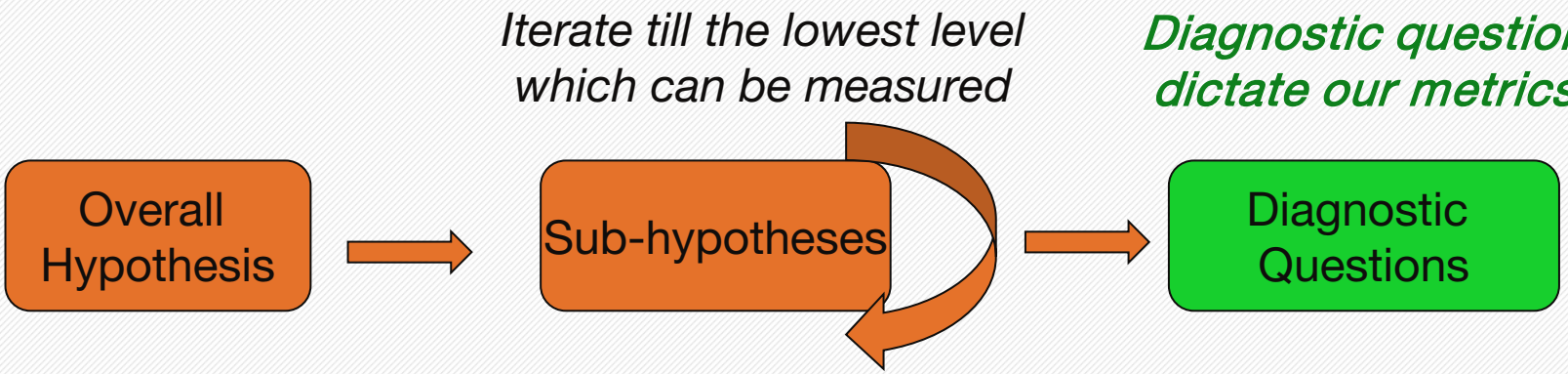
Bad Metrics

- Bad metrics: vague and confusing
  - Inconsistently measured
    - Ratings-oriented “metrics”, they are very useful for “taking organization’s temperature”
  - Cannot be gathered cheaply (expensive metrics)
    - For metrics that are more operational or diagnostic in nature, long sampling intervals will not cut it.
  - Does not express results with cardinal number and units of measure.
    - Subjective scores numeric equivalents – are functionally equivalent to ratings.

Not Metrics

- Security Framework “measurements”, particularly those related to ISO 17799 (10 subject domains, 150 control areas)
  - Many “metrics” project focus on subjective assessments against an established taxonomy.
  - Self-assessment tool designed to quantify risk based on the ISO standard and ALE method.
  - ISO 17799 is a well-structured security taxonomies, and is often used as guidelines for assessing compliance with good industry practices. But NOT a metrics framework.
    - Excessive focus on audit (security control requirements, no practical recommendations)
    - Subjective success criteria (highly descriptive, but rarely prescriptive)
    - Insufficient attention to measurement
- Annualized loss expectancy (ALE)

McKinsey-style “diagnostic”



“The firm is secure from wireless threats by outsiders”.

“Open wireless access points are not accessible from outside the building”.

“There are no open wireless access points that can be accessed from the building’s parking lot or surrounding areas”.

“Wireless access points on the corporate LAN require session encryption and reliable user authentication”.

“100% of the wireless access points on the corporate LAN require 128-bit WAP security.”

Use Metrics to Diagnose Problems: A Case Study

- Barry Eiger, CTO, of a large, well-known maker of high-end consumer electronics.
- Challenge facing: To deploy a series of web-based transactional financial systems for customer order management, loan financing, and customer support services, that connects back to several backend applications, such as SAP, Oracle.
- Barry's questions: *"Is my company's customer data secure from outside attack?"*
  - How difficult it might be for an outsider to penetrate his security perimeter and access sensitive customer data.
  - How good his defense really were
  - How well his company compared to other companies

Diagnostic Metrics in Action (1)

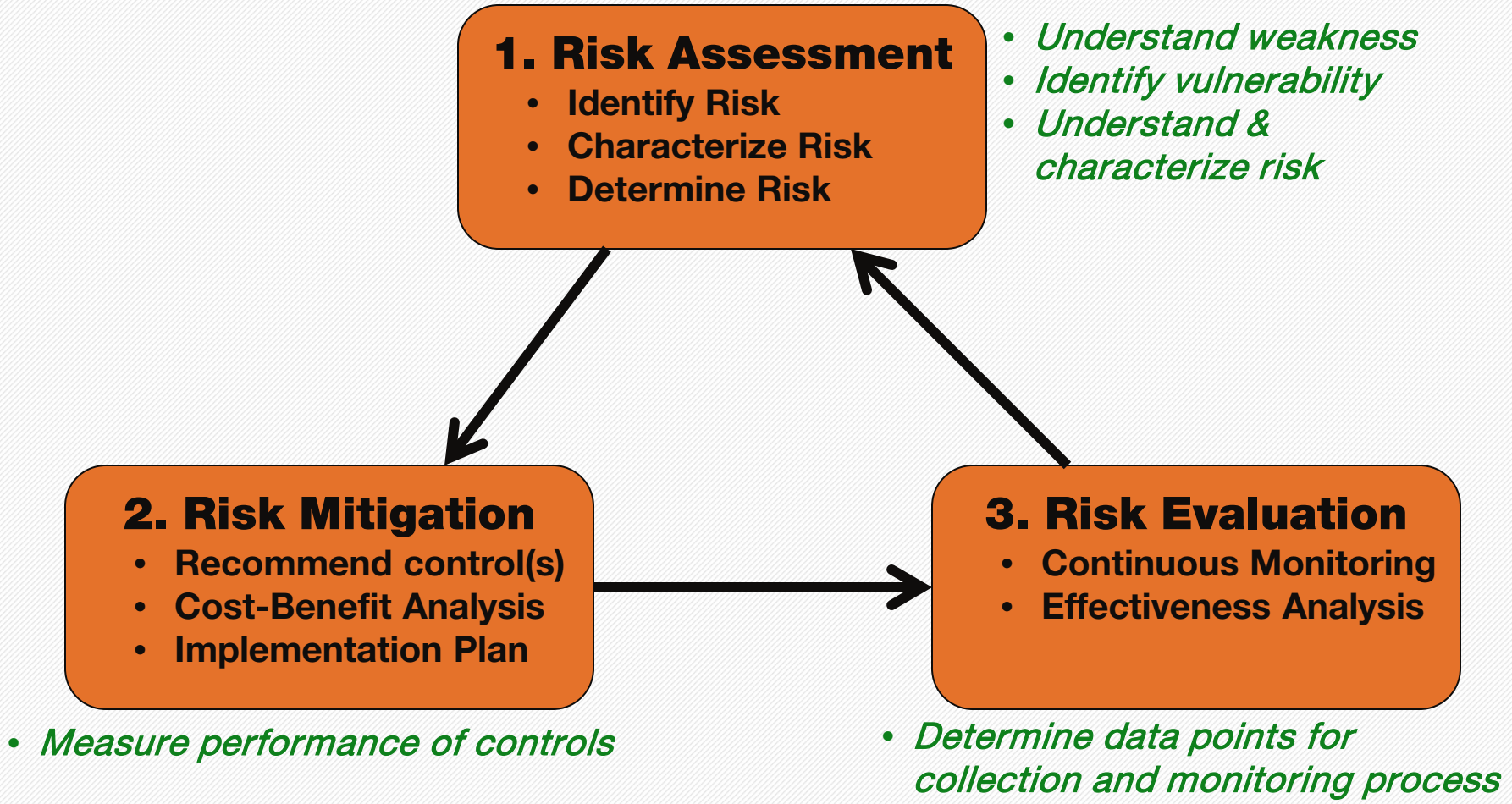
"The Company was highly vulnerable to attacks from outsiders"

- *"The network perimeter is porous, permitting easy access to any outsider"*
- *"An outsider can readily obtain access to internal systems because password policies are weak"*
- *"Once on the network, attackers can easily obtain administrator credentials"*
- *"An intruder finding a hole somewhere in the network could easily jump straight to the core transactional systems"*
- *"Workstations are at risk for virus or worm attacks"*
- *"Viruses/worms can spread to large number of computers quickly"*
- *"Application security is weak and relies too heavily on the "out of box" defaults."*
- *"The firm's deployment of applications are much riskier than those made by leaders in the filed (for example, investment banking)"*

Diagnostic Metrics in Action (2)

- *"The network perimeter is porous, permitting easy access to any outsider"*
  - *How many sites are connected directly to the core network without firewall?*
  - *How many these sites have deployed unsecured wireless networks?*
  - *Starting with zero knowledge – how many minutes are required to gain full access to network domain controllers?*
- *"An outsider can readily obtain access to internal systems because password policies are weak"*
  - *What % of user accounts could be compromised in 15min or less?*
- *"An intruder finding a hole somewhere in the network could easily jump straight to the core transactional systems"*
  - *How many internal "zones" exist to compartmentalize users, workgroup servers, transactional systems, partner systems, retail stores, and web servers.*

Security Metrics in Risk Management Framework



Security Metrics Type (1): Defining Technical Diagnostic Metrics

- Technical metrics:
  - Perimeter defenses
    - Understand the security incidents coming from the outside, measure the effectiveness of antivirus, antispam systems, firewalls, and intrusion prevention systems.
  - Coverage and control
    - Understand the extent and effectiveness of configuration, patching and vulnerability management systems.
  - Availability and reliability
    - Metrics like mean time to recover (MTTR) and uptime percentages show the dependencies between security and profits.
  - Application risks
    - Defect counts, cyclomatic complexity, and application risk indices help quantify the risks inherent to homegrown code and 3rd party software.

Perimeter Security and Threats

- This table shows a representative list of perimeter defense metrics. Most of these metrics should be familiar to most security professionals
  - Emails
  - Antivirus and antispyware
  - Firewall and network perimeter
  - Attacks

Environmental indicator vs. effectiveness measurement

of Spam detected/filtered

Spam not detected/missed

Table 3-2 Perimeter Defense Metrics

Metric (Unit of Measure)	Purpose	Sources
E-mail		
Messages per day (number [#]) • Per organizational unit	Velocity of legitimate e-mail traffic; establishes baselines	E-mail system
Spam detected/filtered (#, percent [%])	Indicator of e-mail "pollution"	Gateway e-mail content filtering software
Spam not detected/missed (#, %)	Effectiveness of content filtering software	Gateway e-mail content filtering software
Spam false positives (#, %)	Effectiveness of content filtering software	Gateway e-mail content filtering software
Spam detection failure rate (%)—not-detected plus false positives, divided by spam detected	Effectiveness of content filtering software	Gateway e-mail content filtering software
Viruses and spyware detected in e-mail messages (#, %)	Indicator of e-mail "pollution"	Gateway e-mail content filtering software Workgroup e-mail content filtering software

Antivirus and Antispyware

Metric (Unit of Measure)	Purpose	Sources
Viruses and spyware detected on websites (#, %)	Propensity of users to surf to sites containing web-based threats	Perimeter web filtering appliance or software
Spyware detected in user files (#) • On servers • On desktops • On laptops	Indicator of infection rate on desktops and servers	Desktop antispyware
Viruses detected in user files (#) • On servers • On desktops • On laptops	Infection rate of endpoints as determined by automated software scans	Desktop antivirus
Virus and incidents requiring manual cleanup (#, % of overall virus incidents)	Shows relative level of manual effort required to clean up	Antivirus software Trouble-ticketing system Manual data sources
Spyware incidents cleanup cost • By business unit	Shows labor costs associated with cleanup	Antivirus software Trouble-ticketing system Manual data sources
Virus incidents cleanup cost • By business unit	Shows labor costs associated with cleanup	Antivirus software Trouble-ticketing system Manual data sources
Outgoing viruses and spyware caught at gateway (#)	Indicator of internal infections	Gateway e-mail content filtering software

Firewall and Network Perimeter

Metric (Unit of Measure)	Purpose	Sources
Firewall rule changes (#) • By business unit • By group's server type	Suggests level of security complexity required by each	Firewall management system Time-tracking and charge-back systems
Firewall labor (# full-time equivalents)	Labor required to support business unit firewall needs	HR management system Manual data source
Inbound connections/sessions to Internet-facing servers (#) • By TCP/UDP port • By server type or group	Absolute level of inbound Internet activity	Firewall management system
Sites with open wireless access points (#)	Suggests potential exposure to infiltration by outsiders	Wireless scanning tools (NetStumbler, AirSnort, and so on)
Remote locations connected directly to core transaction and financial systems without intermediate firewalls (#)	Indicates level of compartmentalization of sensitive business assets, and potential exposure to attack	Network mapping software Network diagrams

Metric (Unit of Measure)	Purpose	Sources
Attacks		
Ratio of Internet web sessions to attackers (%) at three levels of event severity: • Prospects (initial IDS events) • Suspects (machine-filtered/ escalated alerts) • Attackers (manual investigation by staff)	Shows the attack "funnel" by which low-level security events are triaged and escalated, as compared to the overall level of business	IDS Firewall Trouble-ticketing system Manual data sources
Number of attacks (#)	Absolute number of detected attacks, both thwarted and successful	IDS Manual data sources
Number of successful attacks (#, %) • By affected business unit • By geography	Indicates the relative effectiveness of perimeter defenses	IDS Manual data sources

Coverage and Control Metrics

- Coverage metrics measure the security organization’s ability to execute on its mandates.
- Control metrics
  - For the things we’ve got covered, are we getting the results we want?

Coverage and Control Metrics

- Antivirus and Antispyware
- Patch management
- Host configuration
- Vulnerability management

Antivirus & Antispyware

Table 3-3 Coverage and Control Metrics

Metric	Purpose	Sources
Antivirus and Antispyware		
Workstations, laptops covered by antivirus software (number [#], percent [%])	Extent of antivirus controls, for eligible hosts	Antivirus software Network management system
Workstations, laptops covered by antispyware software (#, %)	Extent of antispyware controls, for eligible hosts	Antispyware software Network management system
Metric	**Purpose**	**Sources**
Servers covered by antivirus software (#, %)	Extent of antivirus controls, for eligible hosts	Antivirus software Network management system
Workstations, laptops, servers with current antivirus signatures (#, %)	Service level agreement (SLA) attainment of antivirus	Antivirus software
Workstations, laptops, servers with current antispyware signatures (#, %)	SLA attainment of antispyware	Antispyware software

Patch Management

Patch Management		
Hosts not to policy patch level (%) • For workstations • For servers • For laptops • For critical systems • By OS: Windows, Linux, UNIX, Mac • By business unit • By geography	Identification of gaps in patch management process	Patch management software Vulnerability management system Systems management software

Metric	Purpose	Sources
Unapplied patch latency (age of missing patch, per node)[12] • For critical patches • For noncritical patches • By business unit • By geography	Shows potential size of window of vulnerability for missing patches	Patch management software
Patch testing cycle time (time) • For critical patches • For servers versus workstations • For noncritical patches	Measures time of exposure due to elapsed time between release of official patch and time of completion of patch testing	Patch management software
Patch distribution cycle (time) • For critical patches	Measures time of apply patches	Patch management software
Patches applied outside of maintenance windows (#, %) • For critical systems	Indicates whether control processes are "panicked" or predictable	Change control software Manual controls
Patch SLA attainment (%) • For all systems • For critical systems • Trend versus previous month	SLA attainment for patch management process	Patch management software Vulnerability management system Systems management software
Cost of patch vulnerability group (cost [$])[13]	Total cost of applying a set of patches, including management software, hardware, and labor	Patch management software Time-tracking software

Host Configuration

Metric	Purpose	Sources
% systems in compliance with approved configurations	Shows conformance against configuration standards, regardless of how the system was built	Change control software Desktop management software
Network services ratio (services per host)[14] • All ports • Unnecessary ports • By system type	Identification of potential network ingress points on nodes; suggests divergences from standard builds	Port scanning tools
Remote endpoint manageability (%)	Systems that can be remotely administered by security personnel and that are subject to antimalware and patch management controls	Systems management software Patch management software Antivirus/antispyware software
Business-critical systems under active monitoring (%)	Identifies the extent of uptime and security monitoring controls	Security event management system
Logging coverage (# of nodes, %)	Determines how many hosts forward system and security events to a centralized log server	Systems management software Syslog server logs SNMP traps
NTP server coverage (# of nodes, %)	Determines how many hosts synchronize clocks via a standardized time server	Systems management software Time server logs
Emergency configuration response time (time)[15] • By business unit • By geography • By operating system	Time to reconfigure a given set of nodes in the event of zero-day outbreaks or security incidents	Time-tracking software

Vulnerability Management

Vulnerability scanner coverage (#, %, frequency) • By business unit • By geography • By network or subnet	Shows the extent of vulnerability scanning operations as compared to the total number of IP addresses Frequency measures how often scans are performed	Vulnerability management software

Metric	Purpose	Sources
Vulnerabilities per host (#)[16] • Critical vulnerabilities • By system type • By asset class	Indicates the relative level of potential insecurity based on the number of vulnerabilities per host	Vulnerability management software
Monthly vulnerability counts (#) • By criticality • By business unit • By geography • By system type	Raw numbers that, over time, paint a picture of the overall vulnerability workload	Vulnerability management software
Monthly net change (+/–) in vulnerability incidence • By criticality • Critical assets • Other assets	Shows that change in workload from month to month	Vulnerability management software
Vulnerability identification latency (time)	Shows the degree of responsiveness of the vulnerability triage process	Vulnerability management software Time-tracking software
Time to close open vulnerabilities • For critical assets	Characterizes the level of responsiveness in fixing important vulnerabilities that affect critical assets	Vulnerability management software Trouble-ticketing software
Time to fix 50% of vulnerable hosts (# days), aka "half-life" • For critical vulnerabilities	Identifies the "half-life" of the window of vulnerability for an organization's assets. Measures the effectiveness of remediation activities.	Vulnerability management software
Systems requiring reimaging (# per period, % per period)	Trailing indicator of potential downstream workload impact due to (in)security	Spreadsheets Manual tracking

R·I·T

Vulnerability Management

Metric	Purpose	Sources
Workstation, laptop, server survival (time)	System integrity/survivability; systems with few vulnerabilities should survive much longer	Honeypot software Manual tracking
Time to re-create fully backed-up server from scratch (time as % of SLA)	Efficiency in restoring services to a resource within business requirements	Manual tracking

Availability and Reliability

- The trend: merging of security, availability and reliability.
- Related IT operation metrics
  - Uptime
  - System Recovery
  - Change control (changes to the configuration of the environment)

Uptime

- Planned downtime
- Unplanned downtime
- Uptime
- Mean unplanned outage length
- Median unplanned outage length
- Mean time between failures

System Recovery

System Recovery		
Support response time (average time)	Average time from outage to response	Spreadsheets
Mean time to recovery (time)	Characterizes how long it takes to recover from incidents	Spreadsheets
Elapsed time since last disaster recovery walk-through (days) • For nominated business-critical systems	Shows relative readiness of disaster recovery programs	Spreadsheets Manual tracking

Change Control

Change Control		
Number of changes per period (#)	Measures the amount of periodic change made to the production environment	Change control software
Change control exemptions per period (#, %) • By business unit	Shows how often "special exceptions"are made for rushing through changes	Change control software Spreadsheets
Change control violations per period (#, %) • By business unit	Shows how often change control rules are willfully violated or ignored	Change control software Spreadsheets