Applied Security Metrics

Planning, design and implementation of security metrics

Doug Streit, ODU
Dan Han, VCU

Designing a Security Metrics Framework

Doug Streit, ODU

Metrics Program – Getting Started

1. Add metrics to someone's position
   - IT Security roles are not always defined
   - There will be some care and feeding
   - It needs to be viewed as important

Metrics Program – Getting Started

2. Initiate a project
   - Identify basic targeted metrics
     - Demonstrate key initiatives
     - Demonstrate value on an investment
     - Support an awareness effort
     - Establish performance benchmarks
     - Support already existing audit monitoring

Metrics Program – Getting Started

3. Gathering and presenting the data
   - Identify tools that are available
     - LanDesk, McAfee ePO, FireEye, SpamTrap, Logs, SIEM
   - How can each tool be utililized?
   - Are there built-in graphs or reports?
   - Are there built-in exports that can be used?
   - How do we want to present the metrics?
   - Are there special skill-sets needed?

Metrics Program – Getting Started

Building a framework:

- Graphite stack:
  - Whisper (fixed size DB)
  - Carbon (metrics importer\listener)
  - Graphite (graphing)
  - Diamond (optional agent)
- Web front – web app inside Python (Django)

Metrics Program – Getting Started

4. Prioritize
   - Ease of development
   - Necessity
   - Value
   - Comprehensive wish list

Metrics Program – Getting Started

5. Make a short-term plan
   - Biting off too much will stall the effort
   - Is there a current initiative?
   - Where can you find a quick win?

Metrics Program – Getting Started

6. Make a long-term plan
   - Before finalizing the short-term goals, map out long-term possibilities
   - Plan to meet periodically
   - Keep running tab on progress

Metrics Program – Getting Started

7. Schedule a brief with the CIO
   - Once the short-term is in sight
   - Create a deadline
   - Demo to key stakeholders – CIO, Directors
   - Demonstrate value in the effort

Designing and Implementing Security Metrics

Dan Han

When I first started in this role, I asked my Sr. VP what his expectation is for Information security.

His answer?

YOU KNOW SOMETHING?
NO SURPRISES FOR YOU!

The mission: minimize the risks of surprising my superiors

The VCU Information Security Office strives to protect the security and privacy of VCU constituents by monitoring, detecting, assessing, preventing and reporting on threats that target the sensitive information of VCU constituents. Further**, VCU Information Security Office strives to protect the integrity and reputation of the University and minimize any legal, financial and reputational costs incurred from information security related issues.** Finally, the VCU Information Security Office aims to provide security awareness within the community to better equip the citizens of our society with tools to better recognize, prevent and mitigate threats and risks in information security.

But How?

More questions than answers

- What are our goals and objectives?
- What are we trying to protect?
- Why are we protecting it?
- Where does it reside?
- Who are we protecting it from?
- What are we protecting it from?
- How can we protect it?

It didn’t take long for me to recognize

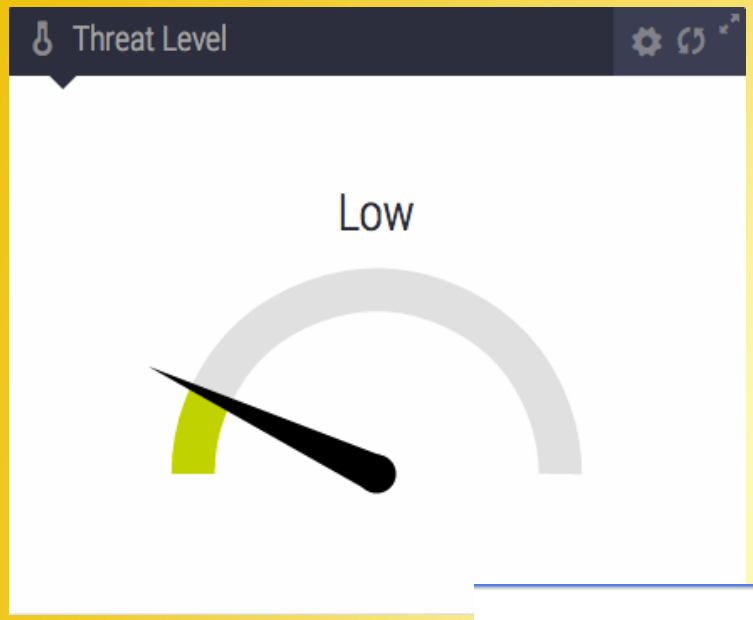
- Need to understand
  - Assets (Location, Sensitivity)
  - Threats (Capability, Probability, Targets)
  - Vulnerabilities (Trends, Lifecycle management)
  - Countermeasures (Effectiveness, Cost)
- Leverage this information to derive a risk profile for the effective management of risks

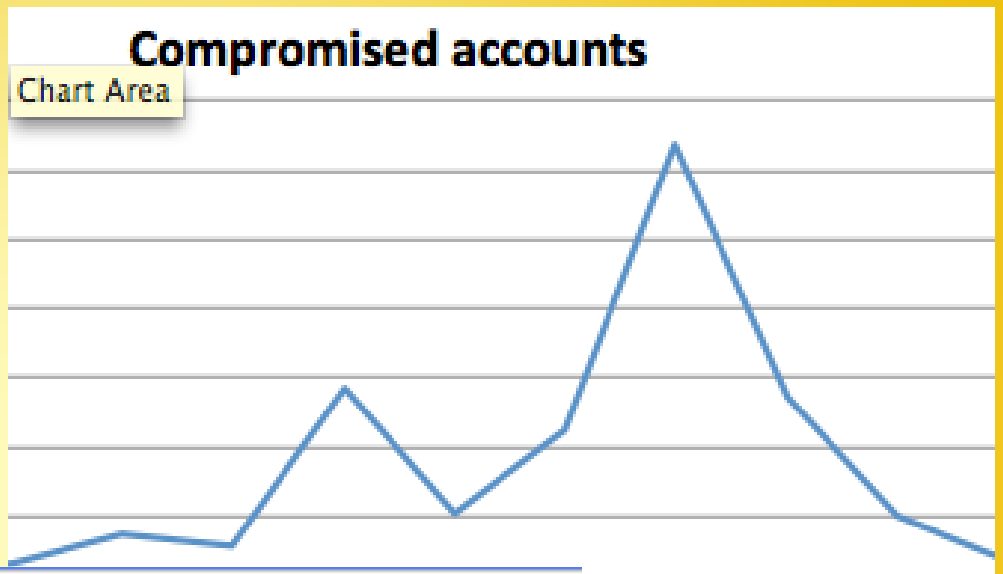
Purpose of Metrics

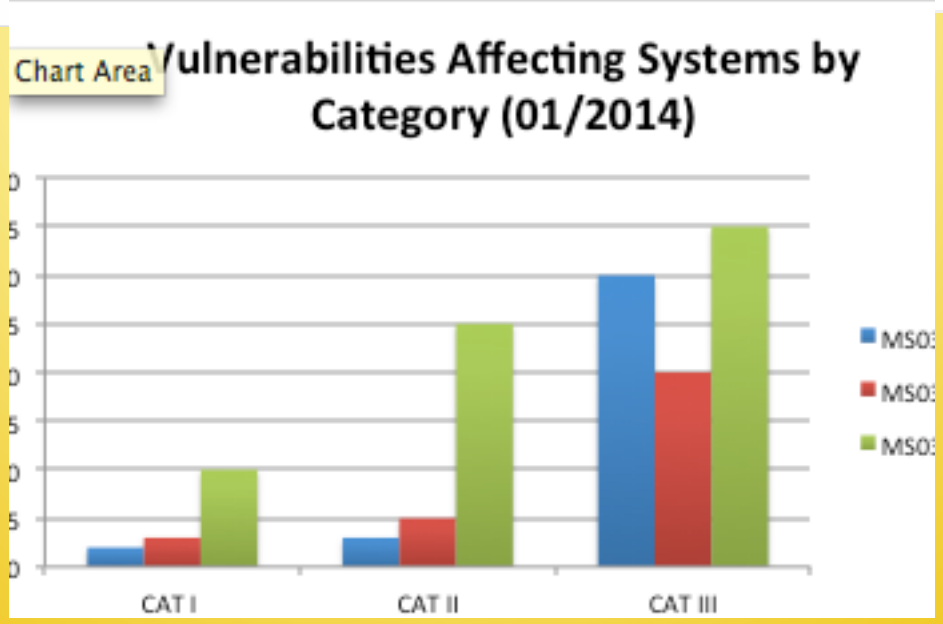
- Strategic and tactical planning and management
  - Risk identification, classification, and management
  - Benchmarking
  - Allocation of resources to appropriately manage risks
- Countermeasure effectiveness assessment
  - Measurement of threat reaction to countermeasures over time
- Reporting
  - Provide performance / statistical information to management and / or community.

Meaningful metrics?

Which one of these metrics is the best?







Meaningful metrics…

- Meaningful to whom?
  - Security engineers
  - Security management
  - IT management
  - Business management
  - Business staff
  - Customers
- No “one size fit all” metrics, need to be developed for your audience.

In other words…

- CISO / Security Operations managers
  - Detailed threat / vulnerability trending data
  - Correlation data between threat / vulnerabilities / assets
  - Detailed countermeasure performance trending data for all countermeasures
- CIO / CISO
  - Business / IT performance data
  - Summarized trending threat / vulnerability data affecting core assets
  - Mid – long term countermeasure effectiveness data
- CEO / CFO
  - Summarized business / financial impact data
  - Supporting trending data
- Board level metrics:
  - A big button that glows green, yellow, or red / or a meter that goes from green to red
  - Limited summary trending data

Effective metrics

- Must have clear definitions (e.g. incident vs. intrusion attempt)
- Should support repeated collection over repeatable and logical means
- Should be consistently collected
- Should support trending
- Should be comparable to industry benchmarks
- Holistic is better than atomistic
- Objective is better than subjective
- Quantitative is better than qualitative
- Automated is better than manual

The $204 / record breached cost

- The Ponemon cost of data breach number
- How would you use this number with your CFO or equivalent?
  - Number is taken from multiple countries across various industry verticals with variance among verticals
  - 68% of the cost associated with US data breaches is attributed to indirect costs (in 2013)
  - What about fixed versus variable costs? Marginal (per capita) cost should decrease with the increase of number of records breached!

The point is, effective metrics must be…

Collected using justifiable and defensible methodology

and

<u>Used properly</u>

What do you want to know?

- Don’t collect for the sake of collecting, metrics must have purpose
- Consider the evaluation of your information security management program first
  - Define program functions (e.g. incident handling, intrusion detection, risk management, training & awareness, governance, etc)
  - Identify useful KPI for each function

CMMI measurement

Information Security Planning Session (2011 - 2012)						
CMMI Le	**Description**	**Incident Handling**	**Intrusion Detection & Monitoring**	**Risk Management**	**Security Training and Awareness**	**Governance**
Level 0	Blissful ignorance					
Level 1	**Initial:** Reactive Ad-hoc processes	Current: 1	Current: 1		Current: 1.5	Current: 1
Level 2	**Managed:** Developed policy set Initiated strategic program Designed architecture	1 year goal: 2		Current: 2.5	1 year goal: 2.5	1 year goal: 2.5
Level 3	**Defined:** Formal definition of processes Organization follows process Basic automation Formalized change control Internal metrics Documentation of		1 year goal: 3	1 year goal: 3		
Level 4	**Quantitatively Managed:** Active and automated tracking of technology and business change Management by Objective	**Final Goal:3.5**	**Final Goal 3.5**	**Final Goal: 4**	**Final Goal: 4**	**Final Goal: 3.5**
Level 5	**Optimizing:** Process Improvement					
Related processes (Documer		~ System Compromises (Server /Workstation) ~ eDiscovery Acquisition ~ Forensic Analysis (process per type, e.g. policy violation, intrusion, etc) ~ Phishing handling/remediation ~ Account Compromise ~ Prioritization/Triage ~ Incident Reporting	~ Intrusion Analysis process (from initial alert to incident declaration) ~ Define what is monitored (Monitoring Criteria) ~ Prioritization/Triage	~ Assessment Targeting (who/what to assess) ~ Assessment/Remediation Processes by type (Business Unit, System, etc) ~ Vulnerability Assessment/Remediation ~ Review/Approval process (scheduled re-assessments, etc) ~ Exception Request Review Process ~ Assessment Prioritization/Triage	~ Training Request process ~ Awareness Assessment Process ~ Training Delivery process ~	~ Change Control for Monitoring Tools (Qradar, SecureSphere, etc) ~ Policy & Standards development (prioritization, etc) ~ Policy/Standards Approval Process ~ Policy Review/Revision Process ~ Policy communication/publication ~ Needs identification/prioritization (technical & administrative) ~ Needs Analysis & Review (based on business & technical needs)
Key Performance Indicators						% of Policies/Standards Reviewed
Internal Performance Metrics		~ # of Incidents Declared ~ # of Indicents Resolved ~ # of Incidents by Type (Malware, Hacking, Social Engineering, Misuse, Physical, Error, Environmental [categories from Secion 2.2 of VERIS Framework]) ~ # of Incidents by Agent (External, Internal, Partner) ~ Time to Response to Incident (time from initial report/declaration to start of incident handling process) ~ Time to Resolve Incident ~ Cost of Incident ~ Target/Victim of Incident ~ Date/Time of Incident Reported/Declared	~ # of Events ~ # of Offenses (Suspected Intrusion Attempts) Reported by Qradar ~ # of Offenses from other sources ~ # of Offenses Investigated ~ # of Incidents Declared ~ Time to Investigate Offense (from start of analysis to resolution) ~ # of Malware attacks detected by Antivirus ~ # of Malware attacks detected by other sources/tools	~ # of Unit Assessments Initiated ~ # of Unit Assessments Completed ~ # of System Assessments Initiated ~ # of System Assessments Completed ~ Time to Complete Unit Assessment ~ Time to Complete System Assessment ~ # of Risks Identified (by criticality, e.g. high/medium/low) ~ # of Risks Remediated (by criticality, e.g. high/medium/low) ~ # of Exception Requests (Denied /Approved)	~ # of Training sessions requested ~ # of Training sessions completed ~ # of Offenses/Incidents reported by end users & tech staff ~ # of InfoSec events? ~ # of Attendees at hosted InfoSec events (by attendee type?) ~ # of employees who completed online awareness	~ # of Policies/Standards reviewed ~ staff time spent reviewing policies/standards ~ Time to approve & publish standard (from initiation to approval and publication) ~

Benchmarking

- It is important to measure yourself against others, especially others in the industry, but to do so…
  - Common framework of measurement
  - Consistent definition
  - Know what to measure and how to collect

YOU KNOW SOMETHING?
NO SURPRISES FOR YOU!

Mission: no surprises

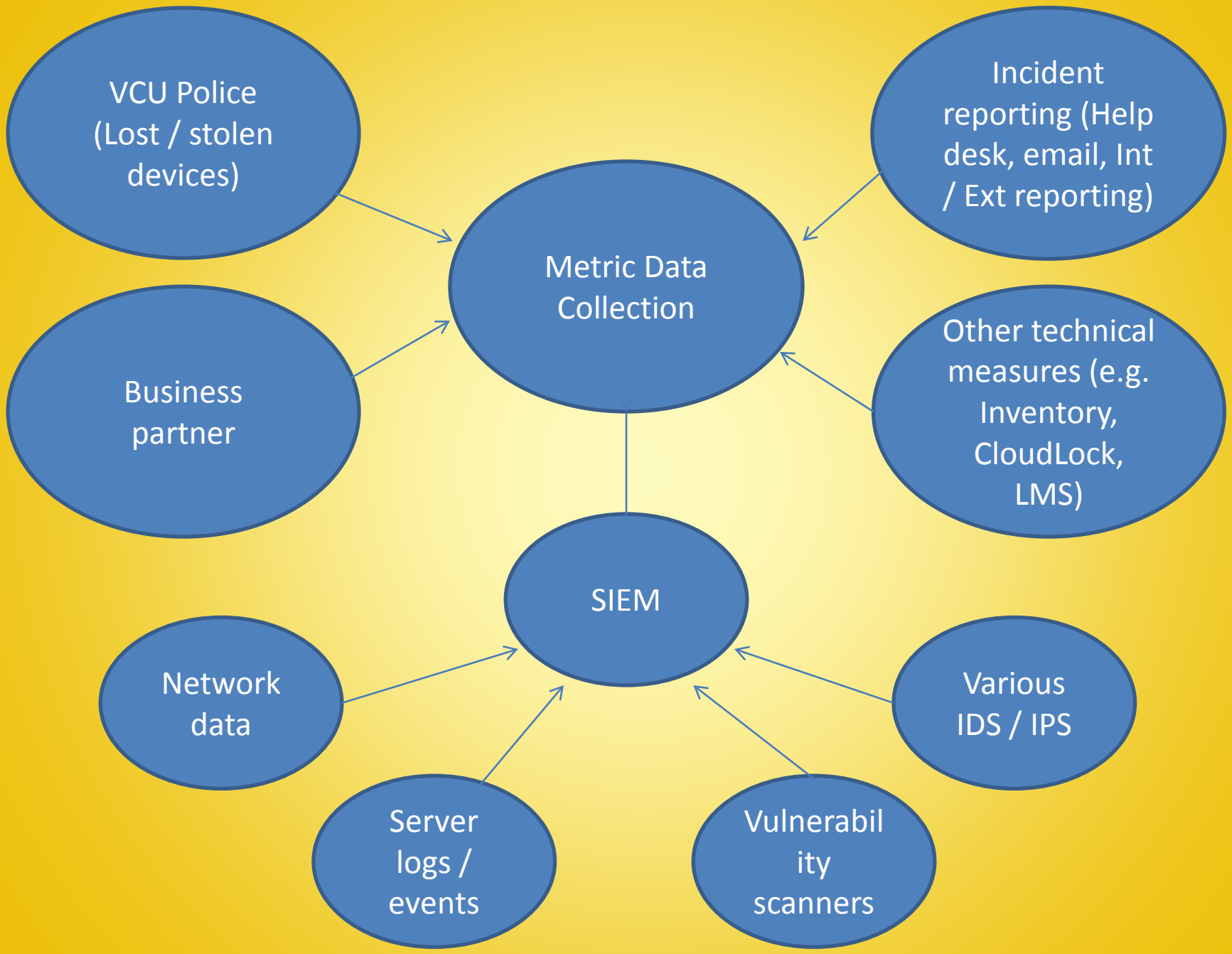
- Goal: Minimize chances of data breaches
- Step 1: Identify and classify the threats
  - Use a common framework
    - **Privacy Rights Clearinghouse**
    - Open Security Foundation Dataloss DB
    - VERIS framework
    - Ponemon

Mission: no surprises

- Step 2: Establish a common set of definitions for metrics
  - Incidents vs. Intrusion Attempts vs. False-positives
  - Breach vs. Near-misses vs. Incidents
  - Active threats vs. Passive threats

Mission: No surprises

- Step 3: Determine the most effective methods for collecting metrics for…
  - Unintended disclosure (Human error)
  - Hacking and Malware
  - Payment card fraud
  - Malicious insider
  - Physical loss of non-electronic information
  - Loss of portable devices
  - Loss of stationary devices
  - Unknown


VCU Police (Lost / stolen devices)
Incident reporting (Help desk, email, Int / Ext reporting)
Metric Data Collection
Business partner
Other technical measures (e.g. Inventory, CloudLock, LMS)
SIEM
Network data
Various IDS / IPS
Server logs / events
Vulnerabil ity scanners

Mission: No surprises

- Step 4: Establish processes for metric collection
  - Automate as much as possible (GRC may help)
  - Meet with other business units and arrange the collection of data
    - Buy-in from other units / individuals must be achieved
    - Criteria for collection of data should be objective and fixed
    - A consistent collection process should be written into procedure

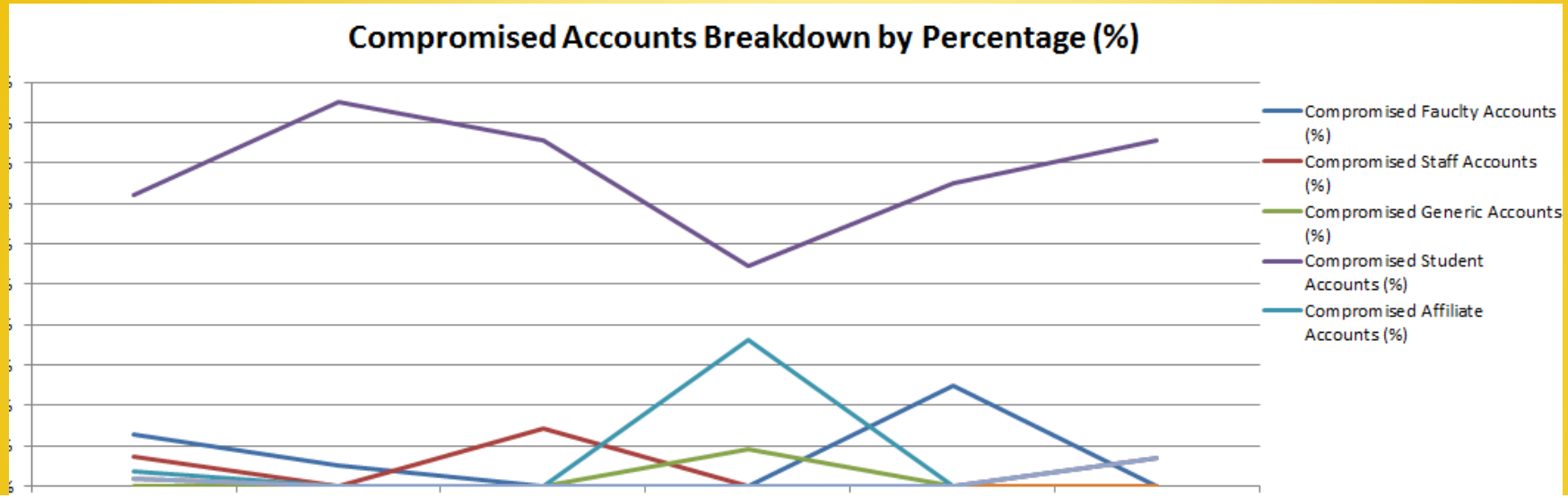
Mission: No surprises

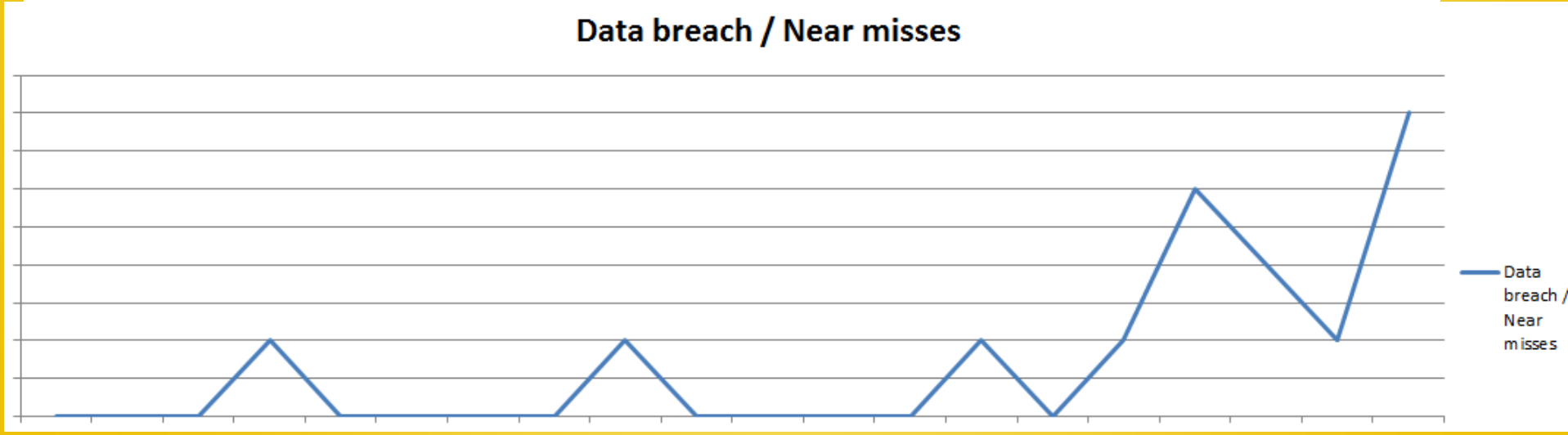
- Step 4: Record and correlate your metrics
  - For security program management
    - Measure the risks of your incident category based on impact to business
    - Measure actual breaches or near-misses (Not Incidents!) against framework data to identify gaps.
  - For countermeasure effectiveness management
    - Obtain incident / threat baseline before implementation of countermeasure.
    - Measure incident / threat data trend over time

Mission: No surprises

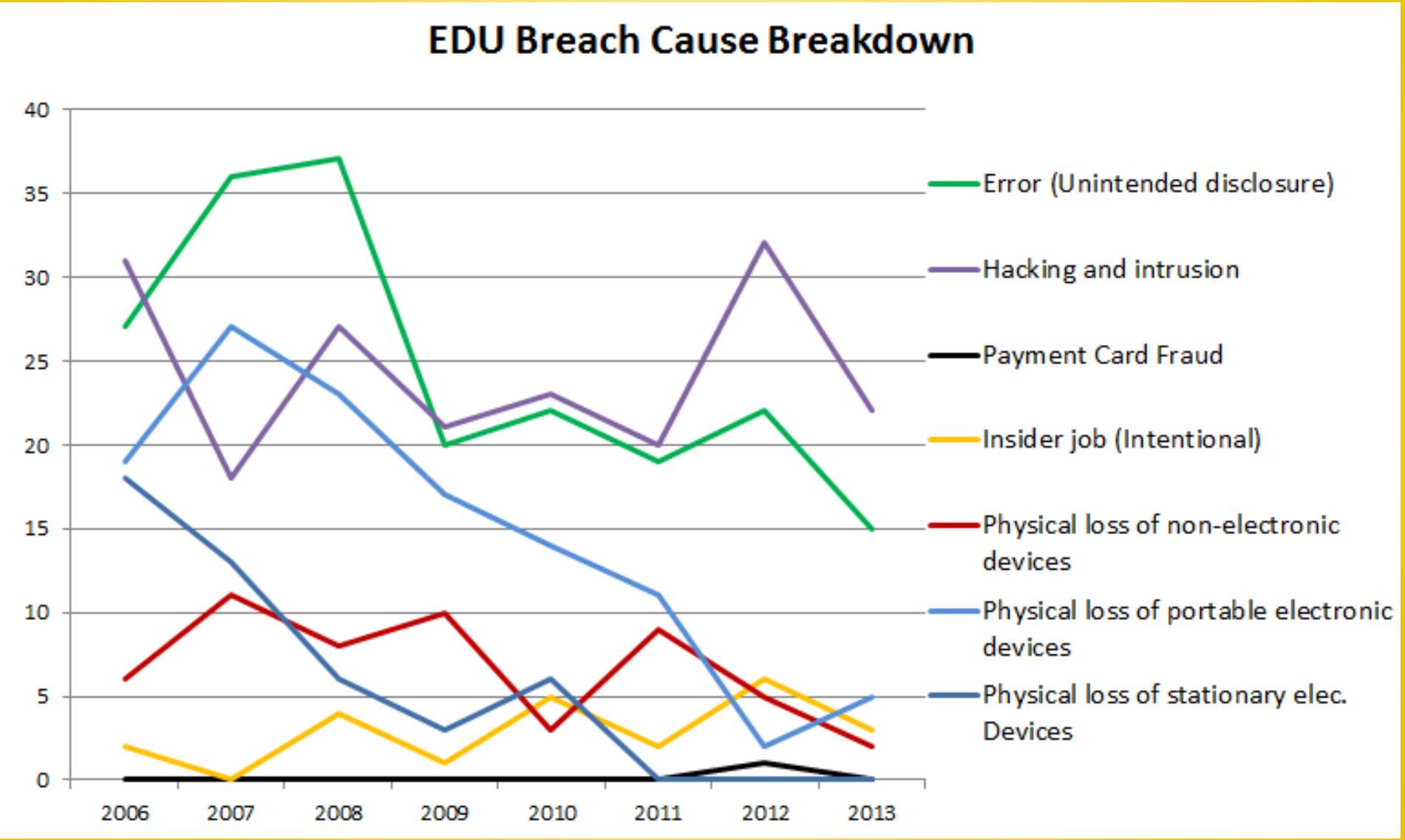
- Step 5: Monitor / review / report and keep it up-to-date
  - Summarize this information on periodic intervals
  - Use graphs (or not)
  - Establish a baseline for your environment, measure your baseline against a framework
  - Triage and investigate anomalies
  - Provide “meaningful” metrics to each levels of the organization.

Ooo… Pretty pictures





More pretty pictures…



Sample metrics

- Threat and incident
  - **Incident experienced per month based on type** (*Allows trending of incident data over time*)
  - **Incident : near miss / breach ratio based on type** (*Allows the identification of riskiest incident types*)
  - **Number of compromised accounts based on affiliation** (*Allows the identification of problematic end user groups*)
  - **Number of lost / stolen devices based on device type / ownership** (*Allows the identification of problematic endpoint groups*)

Sample metrics

- Vulnerability management
  - **Number of Active (exploitable) vulnerabilities affecting sensitive IT systems** (*Allows the identification and trending of possible threats*)
  - **Number of Active vulnerabilities affecting OS or Application** (*Allows the identification of issues affecting IT systems*)
  - **Number of repeating vulnerabilities affecting the same IT system** (*Allows the identification of problematic / high risk systems*)

Sample metrics

- Performance / Countermeasure management
  - **Average time taken to respond to an incident affecting sensitive asset** (*Measures incident response efficiency / capability*)
  - **Number of scams reported to security office** (*Measures community awareness level of your security program*)
  - **Number of compromised accounts based on affiliation** (*Measures the effectiveness of your training program on each end-user community*)
  - **Incident : Trending of number of intrusion attempt by category** (*Measures effectiveness of countermeasures against a particular category of threat*)

Summary

- Metrics must have a purpose, define the purpose first.
- Benchmark yourself against a common metrics system (VERIS, PRCH, Dataloss.DB)
- Metrics must be consistent, and definitions must be consistent, and they must be justifiable and used properly
- Automate collection as much as possible and get buy in when needed
- Investigate anomalies in collected metrics
- Use appropriate metrics for reporting at different levels

Thank you

Questions?