Leveraging Your Tools for Better Compliance

Using People, Process, and Technology to Measure Compliance
Agenda

- Why are we doing it?
- Current Sources of Information (People, Process, Technology)
- Limitation in current Approach
- What makes a good metric?
- Gathering Information
- Analyzing and Presenting Information
- Communicating Results within your Organization
- Summary and Questions
Before we Get Started…

- Who’s Dave, and why should you listen to him?
  - Founder of Sentry Metrics, company with a specialty in working with metrics, key focus on compliance and visibility
  - 18+ years in information security
  - 7+ years helping mid-size to enterprise organizations create policies, metrics, and dashboards
  - 12+ years presenting at shows just like this one, sharing lots of information, war stories, answering questions, educating
  - All-around nice guy! 😊
Why are we doing this?

- Drivers for measuring include:
  - Compliance to standards (PCI, SOX, Bill 198, HIPPA, PIPEDA, etc. etc.)
  - Measuring effectiveness of existing security controls (are we following our defined policies, processes, procedures)
  - Measuring Effectiveness of existing security TOOLS (are they doing what we bought them for in the first place)
Why Should we bother?

- Inability to provide concrete answers to senior management, internal/external auditors, Regulatory Bodies
- Called out on an audit / Failed Audit (can you say not good?)
- Increased scrutiny (can create a BOHICA situation)
- Ability to genuinely say you’re following Best Practices, and have the evidence to back it up
- Be the “Information Guru” within your company (almost like being the life of the party!)
Where do we get our information from today?

- Security Tools (Consoles, Alerts)
- Incident/Ticketing Systems, Change Management Systems
- SIEM Solutions (Security Tools)
- GRC Tools (ESM, Archer, Agilent, etc.)
- Management Reports (manually created)
- Outsourcers (Monthly SLA reports, Incident Reports, etc.)
- Manually Gathered (from employees and other sources)
Let’s Look at Some of the Tools

- Tools tell us only about what they can see.
- Tools aren’t typically designed to talk to each other, or to understand what our other tools are doing (lack of contextualization).
- Without an aggregator (such as a SIEM), tools are operating in isolation and don’t provide adequate visibility.
- Even with a SIEM, it’s only as good as the information it receives, and with its ability to actually do something with the information.
- Very few tools can actually make dynamic decisions based on contextualization of aggregated information.
- Tools are bought to satisfy a security or compliance requirement, but are almost never tested for effectiveness.
Firewalls

- Top 10s
- Top Sources
- Top Destinations
- Top Ports
- Top Protocols

- Limited Visibility into security violations (we see the traffic, but typically not the data/content)
Intrusion Detection/Prevention

- Top Sources, Destinations
- Unique Signatures
- Blocked Events
- Packet Captures of Traffic for forensic purposes
- Lots of information on what MIGHT be happening, but requires time to validate (time=people)
- Has to see what’s going on in order to be able to alert on it and block where necessary
Anti-virus, Anti-spam

- Recent Viruses
- Top Viruses
- Virus Sources
- Infected Hosts
- Quarantined Files

- Limited in most cases to what the deployed AV solution knows about
Data Leakage Protection (DLP)

- Sensitive Data at Rest
- Sensitive Data in Motion
- Data leaving the organization
- Data prevented from leaving the organization
- Which user did what and from where
- Relying on fingerprinting the network, understanding where the data is in the first place
Incident / Ticketing / Change Mgmt. Systems

- Time to Identify an incident
- Time to Respond
- Time to Resolve
- Solutions/Remediation Proposed
- Reason for Incident/Change Mgmt. Request
- Effectiveness of Solution
- % of Roll-back

All items above can only be tracked if an incident is created in the first case, and the ability exists to track it through to completion and audit it.
SIEMS, GRC Tools, Management Reports

- # of Alerts, Correlated Events, Events per Device Type, etc.
- Reports on Activity (user, system, security)
- Events over time (Trending)
Next Steps: Working with the Information

Now that we have a good understanding of many of the data sources, how do we leverage them?
Biggest limitation with most point solutions?

“You don’t know what you don’t know”

- If the tools aren’t aware of what a violation is, they can’t detect it, they don’t identify it, and ultimately you don’t see it.
Next Deep, Thought-Provoking Point

“You Can’t Manage What You Can’t Measure”
What Should we be Measuring

- Overall Effectiveness of the Tools
- Incident Response Effectiveness
- Alignment of Controls to Compliance Requirements
- Effectiveness of Implemented Remediation Recommendations
- SLAs (Internal, External)
- Application Performance
- Infrastructure Performance
Other Considerations

- KPIs, Metrics, and information sources that
  - Align with Risk
  - Assist in determining effectiveness of controls
  - Provide visibility into the overall security posture
  - Are objective, quantifiable, repeatable
  - Allow us to attain and maintain compliance to a standard (PCI, SOX, etc.)
  - Can be summarized, “rolled up”, to contribute to overall compliance status
Aligning Information Sources with Needs

- Review existing policies, regulatory requirements
- Create a matrix of requirements (from audit, from standard, from information security policies, etc.), these become your Controls
- Determine what compliance/non-compliance for each Control actually looks like (Yes/no, threshold, etc.)
- Create an initial baseline for each Control (Yes=Compliant, >80%=Compliant, Response Time > 15 mins=Compliant, etc.)
- Identify a data source (or sources) where you can query information that will help determine compliance
- Identify an Owner, Contributors, and optionally Approvers for each Control
How Do we Analyze the Information?

- Spreadsheets are your friend (highest probability of success)
  - Can easily modify results based on review
  - Easy to create sample graphs, reports
  - Easy to add in additional metrics over time
  - Easy to create complex dashboard views without special tools
Sample Excel-Based Compliance Dashboard

![Excel Dashboard Image]

### PCI v.1.2.1 CONTROL OBJECTIVES FOR

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1.1</td>
<td>Establish firewall and router configuration standards</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
</tr>
<tr>
<td>11.1.2</td>
<td>Verify that there is a formal process for testing and approving of all network connections and changes to firewall and router configuration standards</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
</tr>
<tr>
<td>11.1.3</td>
<td>Ensure the firewall is properly configured</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
</tr>
<tr>
<td>11.1.4</td>
<td>Configure changes to firewall and router configuration standards</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
</tr>
<tr>
<td>11.1.5</td>
<td>Ensure that the firewall configuration standards include requirements for a firewall at each Internet connection and between any DMZ and the internal network</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
</tr>
<tr>
<td>11.1.6</td>
<td>Ensure that the firewall configuration standards include a description of access rules</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
</tr>
<tr>
<td>11.1.7</td>
<td>Ensure that the firewall configuration standards include a document of services, protocols, and ports necessary for business—e.g., HyperText Transfer Protocol (HTTP) and Secure Sockets Layer (SSL) (HTTPS)</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
</tr>
<tr>
<td>11.1.8</td>
<td>Ensure that the firewall configuration standards require review of firewall and router configuration standards at least every six months</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
</tr>
</tbody>
</table>

© 2010 Sentry Metrics Inc.
Why the “Manual Approach” Succeeds

- Gives you the opportunity to try out lots of different ways of modeling your information
- Cost-effective
- Easy to modify, update, add in new metrics
- Easy to simulate the drilldowns without having to build portals
- Doesn’t require expensive hardware, software, support time
- Can be brought online and demonstrated to other interested stakeholders almost immediately
Communicating Compliance to the Organization

- High-level dashboards
- Summary information (50,000 level), show Yes / No
- Granular Access Controls to information (who can see what, and when can they see it)
- Have Drill-down options available to get to original data source whenever possible (evidence, justification/verification, audit, etc.)
- Lots of graphs, charts, etc. (people want to see information in many different ways, make sure you have one that works for them!)
- Provide options to “tune” reports wherever possible
- Give them an option to save reports offline wherever possible
A Moment on Scorecards

- Objective, Objective, Objective
  - Measuring an agreed-to set of controls
  - Present information graphically, numerically, statistically
  - Remember the drill-down for appropriate resources
  - Provide ability to look back at previous scores (trending)
  - Provide ability to see the individual results that went in to creating the final score
Summary (What have we Learned Today?)

- Compliance CAN be measured in a repeatable, reliable fashion
- Tools are a key part of the solution
- Visualize compliance in a way that works for YOUR organization, don’t limit yourself to what a particular tool or technology can do
- No use in creating dashboards, scorecards, KPIs, metrics, reports, etc. if no one is going to use it, so make sure they’re actually useful
- Spending the time up-front to identify the audience for your metrics, and how they want to see it, will save a huge amount in the long run and goes a long way towards overall success
- It’s a learning process, and the end result should be flexible enough to change and grow along with the organization
Questions?

Dave Millier, CEO
Sentry Metrics Inc.
416-488-2323 x121
dmillier@sentrymetrics.com