Security Metrics > Specific Examples >

What Is a Reportable Security Violation in Your Organization?

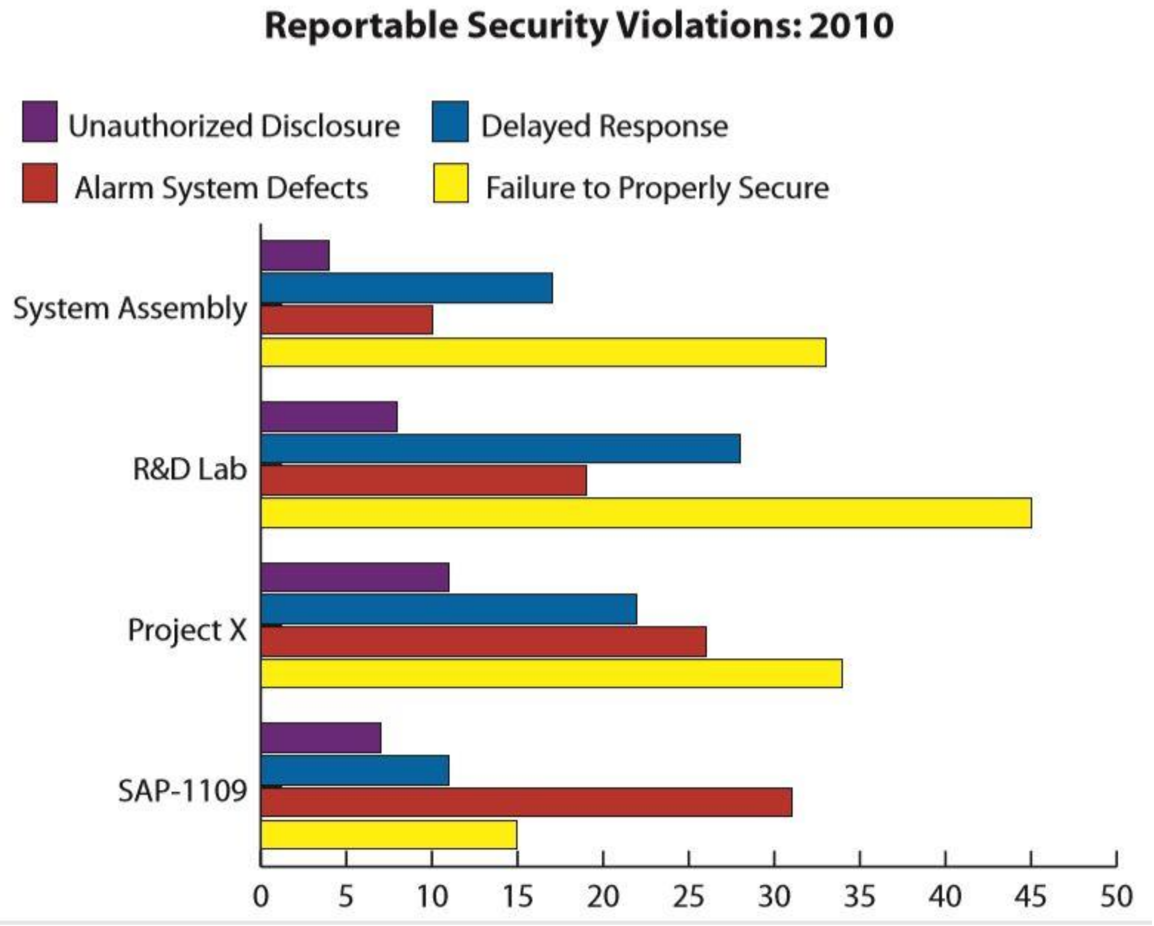
Created by George Campbell, Security Executive Council Emeritus Faculty

How serious is the notion of compliance in your company? Is your reputation in the marketplace linked to conformance to an established set of laws, rules or standards? Are there protection mandates in the contracts you have with your customers and key suppliers? What are the implications of inadequate security with regard to your insurance? We are a key player in the governance of these internal controls.

It's important to track, analyze and report on risk-related conditions and events that are subject to mandated or self-imposed compliance. This helps to identify root causes so as to eliminate defects in safeguards and establish accountability for corrective actions.

Every organization experiences serious compliance events or conditions that must be escalated to a designated individual or authority for notification and remedial follow-up. These are the incidents that make it to the Board's risk management or audit committee. They may require regulatory or customer notification, and they are likely to have noteworthy financial impact. You don't want them on your watch — especially if the failed control belongs in Security's portfolio.

To add insult to injury, most are avoidable. The rules and responsibilities are — or should be — known. The graphic that follows is typical of Security's normal approach to metrics: We maintain counts of what and how much. The essential next step is what security management does with this data. If you accept the fact that what you see here indicates avoidable risks, the next step is to dig deep and uncover the root causes.



Compliance standards all possess embedded measures for monitoring conformance. For example, if certain types of information must be protected to a specific standard, inspections will reveal the status of safeguards, and automated tools and protective systems can monitor for and alert to attempts to compromise protection. Processes to ensure or verify personnel reliability may be measured, as can response to potential threats to protected assets. In sum, there is a diverse inventory of sources for actionable metrics.

In the best of circumstances, an internally directed compliance review or risk assessment identifies the internal control defect or security vulnerability, nails the cause, and addresses the exposure before an event occurs. Your value metric is the number of vulnerabilities you have proactively discovered and fixed. In the worst-case scenario, the defective control that you knew about somehow never got fixed. Somewhere between best and worst is the case in which a previously unidentified defect directly contributes to a notable event. Both of these metrics also need to be tracked—at least, while you are around to track them.

Look at the four indicators being tracked by the department in the graphic above.

• Unauthorized disclosure relates to proprietary information that has been transmitted by any means in violation of standards of protection.

• Delayed response: We can all envision certain types of incidents, alarms or calls for service that establish standards for first responders. Time from dispatch to arrival is logged for verification of adequate response time.

• Alarm system defects: Alarms installed to monitor sensitive areas or assets must meet specific standards of reliability. Standards for tracking faulty, false or nuisance-induced annunciations are checks on system reliability and responder confidence.

• Failure to properly secure relates to the missteps of persons accountable for following established protection standards, whether the cause is malicious intent, negligence, or a flawed understanding of their responsibility.

Think about what is reportable in your company and what protocols are in place to ensure reporting compliance. The rules are clear if you are in a regulated business environment, but may not be in a less formalized setting.

Originally published in Security Technology Executive Magazine

Visit the Security Executive Council website for other resources in the Security Metrics > Specific Examples series.

About the Security Executive Council

The SEC is the leading research and advisory firm focused on corporate security risk mitigation solutions. Having worked with hundreds of companies and organizations we have witnessed the proven practices that produce the most positive transformation. Our subject matter experts have deep expertise in all aspects of security risk mitigation strategy; they collaborate with security leaders to transform security programs into more capable and valued centers of excellence. Watch our 3-minute video to learn more**.**

Contact us at: contact@secleader.com

Website here: https://www.securityexecutivecouncil.com/