

Third Defense helps visualize security risk for financial services

Analyst: Wendy Nather

The problem of analyzing risk underlies nearly all information security practices, regardless of the industry or size of the organization. Risk models abound, from the classic 'frequency times impact equals risk' (which tends to set statisticians' teeth on edge, being the mathematical equivalent of 'peanut butter times jet engine equals shiny') to more refined models such as OCTAVE or FAIR. Every security shaman has a magic risk-analysis formula, and no two are exactly alike, or can even be proven consistently to work. They can't be compared side by side, either, since they can't be communicated in comparable terms. CISOs become frustrated, trying to explain their risk decisions to auditors and regulators as well as to their executive management, and simply describing the risk level as 'orange' or '58.6' doesn't convey enough information.

We spoke with the CTO of one of the largest US-based financial services institutions about its models and processes for analyzing information security risk. The institution asked not to be identified by name, so as not to appear to be commercially endorsing any given vendor product, so we will refer to it here as [Redacted], and to the CTO as 'Alice.' Some of the numerical details have also been tweaked, but are still within the general ballpark to provide context for this report.

Early Adopter Snapshot

[Redacted] is a large financial services firm, with thousands of locations within the US as well as a global presence. It offers numerous types of products to individual consumers, businesses and institutions, using thousands of applications that are either developed in-house or provided by third parties. Its information security activities include incident response, business line threat and risk analysis, technology controls around the operating environment, investigations, IAM provisioning strategy, core security engineering and operations, which is facilitated by a dedicated security budget of over \$50m.

Key areas of innovation

The firm is using Third Defense's Risk Communicator to roll up and rank security metrics; these are used as inputs to the security investment tracking as well as to visualize the overall risk profile at different levels for different stakeholders. It is proving particularly useful for discussing risk decisions with auditors and regulators in a standardized fashion, saving

significant time and resources each quarter.

The 451 assessment

[Redacted]'s risk management program is impressively mature in its consistency and repeatability, thanks in part to the UI from Risk Communicator, which forces the risk enumeration into a standardized language and format. The tool is ideal for those CISOs who treat risk management as both an art and a science; it allows them to tweak data points by hand to achieve the 'right' illustrative relationships. However, the tool would not be suitable for those who believe that numerical formulas should use meaningful units of measurement and be backed up with consistent math, not tweaked to reflect subjective judgments.

Context

As CTO of a firm with a security team exceeding 200, Alice needed to be able to analyze and communicate operational risk using meaningful, repeatable metrics. Together with her CISO, she assembled a set of more than 300 discrete metrics relating to operational security, such as time to patch or exposure window for a vulnerability, and organized them in categories by domain and criticality.

Although these metrics could be tracked in an Excel spreadsheet, the resulting weighting and prioritization were too hard to present to management in that format, and complex groupings of risk factors (such as all the potential issues in an outsourcing arrangement) couldn't be manipulated easily to model risk scenarios. Answering a question like 'What is the likelihood that one of our 20 applications in this business line will be breached?' couldn't be illustrated in an intuitive fashion.

Deployment summary

Alice said that at the time she began building the metrics program, there weren't really any other commercial, off-the-shelf security risk modeling and registry products available, except for those by **Third Defense**, a consulting company founded in 2009 by Jared Pfof and Jonathan Landis. Its suite of risk analysis and management products include the Metrics Manager, Risk Register, Risk Communicator and Service Manager (with the last one allowing a security group to manage its own catalog of security services and resource allocation).

The Risk Communicator proved the most useful to [Redacted], as it allows the security team to track its security investments, map them to metrics outcomes and illustrate its risk management at different levels for different stakeholders – in other words, it bridged the gap between traditional governance, risk and compliance (GRC) tools and the executive boardroom.

Company name

[REDACTED]

Activities

Financial services for consumers, businesses and institutions

Number of employees

50,000+

Key suppliers

Five IDS vendors, two encryption vendors, security services from firms such as Security Compass and Consciere

Strategic vision and business drivers

The financial services firm has made information security risk management into a mature operational process: it releases a risk-based scorecard on a monthly basis, and reevaluates and reprioritizes its metrics and their rankings quarterly and annually. Alice described the environment before Third Defense's Risk Communicator as one where security architects debated security issues in front of the business customer; it was one opinion against the others, without a consistent framework or language. With a shared tool in place that contained business context and standardized vocabulary, the large security team could be 'on the same page' well before any discussions took place with the business lines directly.

It's even more important for a firm to have everyone on the same page when it comes to speaking with auditors and regulators. [Redacted] uses Risk Communicator to describe and defend its risk decisions as they apply to compliance; Alice says the time saved on a quarterly basis with those conversations alone more than makes up for the cost of the tool (averaging \$36,000 for an enterprise license). In comparison with GRC products that appear similar in the marketplace but run up to \$100,000 or more, the annual fee for Third Defense needs no defense.

Challenges and obstacles

A company collecting metrics is often at the mercy of whatever collection of security products it has: whatever they report, in whatever units and format, has to be rolled up somehow and imported for processing. For example, a firewall's log showing a certain number of probes against a port used by a particular application has to be interpreted – is this a high number or not, and what level of threat does it represent? Then it has to be matched with data showing whether any of those probes reached any number of servers on which that port could be active. And then there is the question of whether that application is (or was) running on any of those servers, and whether the application had a known vulnerability during that window of contact. There are no consistent units of measurement that could be used to translate this combined set of conditions into a risk level of 'five'; at every step of the way, the security professional collecting this data has to interpret it and add business context, even if it's something like, 'We see this all the time and we know what it really means.'

The challenge, then, is to add this extant knowledge into the risk visualization so that the values are displayed more accurately. Third Defense's Risk Communicator understands that risk depiction for many CISOs isn't about math, it's about showing relationships using positioning guided by numbers. So the tool allows the user to drag and reposition points on the heat map to convey the information that best represents that user's opinions and interpretation of the risk, overlaid on top of whatever numbers have been collected.

This is a key point of differentiation for CISOs who consider risk management to be an art as well as a science, and who govern by feel as well as by evidence. However, there's another school of thought in security risk analysis that says that using numbers this way, in pseudo-mathematical relationships and including subjective inputs, is misleading at best, so CISOs with a more scientific bent will see this feature of Risk Communicator as a flaw. In a way, the Risk Communicator product neatly highlights a growing dichotomy in the security risk

analysis community: between those who are seeking an objective, evidence-based model, and those who believe that not all risk factors can be captured in a formula.

Innovation and roadmap

As far as it can, [Redacted] is using evidence-based metrics to drive its security risk management, and is using Risk Communicator as a translator to its security stakeholders. It is proving particularly useful to the firm to steer the conversation with its auditors and regulators from a cohort discussion ('Why aren't you addressing this at the same priority level as other financial institutions?') to an actual risk discussion that is grounded in its own business context and professional judgment.

Alice says she suspects these two stakeholder groups in particular will start to demand more structured, standardized risk reports like the ones she's using, and would like to see a similar product adopted more broadly. Third Defense positions itself against custom-built risk management tools written by systems integrators, for example, and it might be able to sell itself to a GRC vendor that wants to expand its reporting capabilities to travel from the oven all the way to the dining-room table.

Reproduced by permission of The 451 Group; copyright 2011. This report was originally published within The 451 Group's Market Insight Service.

For additional information on The 451 Group or to apply for trial access, go to:
www.the451group.com