DERIVATIVETECH™

derivativetech.com

Information security maturity & why it matters

Insight for more efficient and effective information security investment

January 2017
Efe Orhun, Managing Partner
Matthew Archibald, Managing Partner

There is always new information about emerging threats and new information security solutions, but almost all information security problems that damage organizations are not new. According to Gartner, 99 percent of exploited vulnerabilities have been known by security and IT professionals for at least the previous year[3]. Most information security professionals already know the problems facing their organizations—but with limited resources it is difficult to know what to do about all of them.

Determining what needs to be done first requires an assessment of the information security organization. There are many metrics to choose from—in fact, information security is often distracted by the wide array of technical and compliance related metrics available. Technical metrics address vulnerabilities such as mismanagement symptoms, malicious activities, or incident reports, but it can be hard to know which of these issues calls for an all-out response. Compliance-related metrics tend to meet the needs of internal audit and regulatory bodies, but they seldom provide useful data or analytics on the information security organization.

The best metrics are intuitive

To defend against these threats, what you really need is an assessment of your existing information security organization, and insight into how security concerns align with business threats and business objectives. Organizations use qualitative, quantitative, technical, and non-technical approaches plus a variety of other metrics. But the best insight into the health of an information security organization often comes from qualitative, non-technical, simple, and understandable metrics. These can be an accurate and holistic way to measure the strength of an information security organization—and they capture what you need to make a plan and prioritize. Instead of metrics without meaning, look for metrics that are:

- Intuitively understandable.
- Easy to gather and support.
- Consistent and repeatable.
- Aligned with the business objectives of the organization.

Measure maturity

The chief metric that fits all these criteria is the maturity of an information security organization. One way of measuring this is to look at each of the information security organization's areas of activity within your company and align qualitative perceptions with measurements, such as:

- 0 – Not performed
- 1 – Performed informally
- 2 – Planned & tracked
- 3 – Well defined & communicated
- 4 – Managed & measurable
- 5 – Continuously improved

Maturity can and should mean different things to each organization. Experience-based intuition and subjective data are open to interpretation but remain critical ingredients in determining priorities. Your team will have an intuitive sense of the current state of maturity levels within the information security organization.

Derivative Technology
520 S. El Camino Real, Suite 423,
San Mateo, CA 94402 USA

P: +1 (650) 200-3680 F: +1 (650) 240-3638
E: info@derivativetech.com
derivativetech.com

Set your targets

Once you know your current state, set your targets. Assessing maturity levels can inform a philosophy of continuous improvement towards desired goals, by spelling out what level of maturity you should be aiming for, and how to go about achieving it.

A holistic view that looks at Information Security in a business context is the best way to ensure alignment around strategic goals. To connect the Information Security organization with business objectives, bring business and technology together. The target maturity of the information security organization should be tied to not only technical requirements, but also business objectives, the business model, and risk appetite.

Measuring risk is complex, but you can arrive at a strong proxy measurement by identifying areas of impact and their materiality to your business. While no tool can perfectly measure your company's impact profile, weighting key impact areas is a good place to start. They align with risks but can be measured more easily.

Begin by considering the importance of each of these impact areas:

- Information Assets
- Compliance
- Financial
- Geo-location
- Human
- Privacy
- Process
- Reputation
- Technical

These areas have the potential to substantially impact virtually any business, but some will be more significant to your company than others. Prioritize them appropriately to inform your decision making on how to best improve information security. Does the company care about reputation at all costs? Or is privacy king? How about economics? Increase emphasis on the most important, highest-impact areas to align impact priorities with the maturity of the organization and decide what to tackle first.

Information security controls, by design, mitigate impacts. Assigning greater weight to any given area increases the pressure to address the relevant controls. The end result is a view of business-driven information security requirements prioritized by urgency. When information security has created a maturity assessment and a clear business-aligned roadmap then it has the data it needs to decide what to do—and what to do first.

Make your case

Measuring the maturity of an information security organization takes time and requires the input of multiple stakeholders. At the conclusion of the process, you should have a holistic view that puts information security in a business context to ensure alignment around strategic goals. Now you're ready to:

Derivative Technology
520 S. El Camino Real, Suite 423,
San Mateo, CA 94402 USA

P: +1 (650) 200-3680 F: +1 (650) 240-3638
E: info@derivativetech.com
derivativetech.com

- **Communicate better**: Demonstrate that the information security team understands the pain points of the business by connecting and correlating information security activities to their business impact.
- **Improve productivity:** Focus the information security organization on the most urgent requirements and increase efficiency by concentrating limited resources on important tasks such as incident response and innovation.
- **Target spend:** Partner effectively with the business by showing the value created by investing in information security.

For more information
Specialized software and information security risk experts can help your organization to measure its current maturity and create its own roadmap for improving security in alignment with the priorities of the business. For more information, please see the Asena Solution Brief available at http://asena.derivativetech.com, or talk with a Derivative Technology information security and risk professional.

About Derivative Technology
Derivative Technology (www.derivativetech.com) is a Silicon Valley-based information security and risk management consultancy established in 2002 to provide balanced custom solutions that use industry leading practices and address each challenge from multiple perspectives, including people, process, technology, and risk. The Derivative Technology team brings multiple decades of experience in all aspects of IT business processes, information systems operations, security & risk management, and regulatory compliance together to deliver measurable, timely, and sustainable value. We serve various sizes of companies globally, focusing our efforts on the following areas:

- Cyber security threat analysis and countermeasures
- Business continuity and disaster recovery
- Maturity and capability measurement
- Business process design and risk assessment
- Infrastructure operations, security, and risk assessment
- Security incident response services
- Secure solution design

Derivative Technology
520 S. El Camino Real, Suite 423,
San Mateo, CA 94402 USA

P: +1 (650) 200-3680 F: +1 (650) 240-3638
E: info@derivativetech.com
derivativetech.com