SATORI CONSULTING

SCENARIO-BASED CYBERSECURITY ASSESSMENT

Leading cybersecurity standards, such as ISO27002, are typically assessed using standards-based questionnaires to confirm successful implementation of controls and processes. While the current approach is useful, organizations are now looking for ways to further harden security by taking account of their specific business critical processes, and the types of threat posed to them.

Satori's scenario-based cybersecurity assessment augments traditional assessments through in-depth analysis of business processes, identifying the highest impact risks to applications and infrastructure. Result are used to prioritize investments and minimize cybersecurity risk.

New York, 212.918.4560

Satori CONSULTING

info@satoriconsulting.com

THE CHALLENGE

Satori's Scenario-Based Cybersecurity Assessment helps an organization prioritize initiatives to address the cybersecurity challenge:

It isn't an understatement to say that there is a cybersecurity crisis facing many industries. The "dark web" provides a ready marketplace for the sale of sensitive personal and organizational data to bad actors who use it for purposes of fraud, theft, industrial espionage, political manipulation… the list goes on. Any organization that stores and processes information is a target, and much more so if the data include personally identifiable financial or health information.

At the same time regulators, such as the Bank of England, are becoming increasingly concerned about the interconnectedness of systems and processes across organizational (and often international) boundaries. These interconnections create hidden fragility in complex systems, where a seemingly innocuous failure in one organization can cause downstream failures (that may be much more catastrophic) elsewhere in the overall business process. Cybersecurity events, such as denial of access or denial of service, are major sources of this type of failure.

These concerns have led to the burgeoning industry in cybersecurity assessments. Leading cybersecurity standards, such as ISO27001 are usually assessed using questionnaires based on COSO or COBIT standards that codify Best Practices for processes and controls. These assessments are undoubtedly useful, but they don't take account of the risk profile of specific industries or the threats posed to organizations' specific business processes, applications, infrastructure, and the interconnectedness to other industry players.

Organizations are beginning to implement scenario-based assessments to investigate chains of cause-effect and expedite actionable improvements. However, scenario-based approaches to date have usually focused on simulations of specific cybersecurity events over hours or even days. There are challenges with this approach because the simulations are costly to run and may focus unduly on just the threat simulated.

NIST Security Framework

THE SATORI APPROACH

Satori's scenario-based cybersecurity assessment augments traditional assessments through in-depth analysis of business processes, identifying the highest impact risks to applications and infrastructure with reference to the NIST Security Framework. Result are used to prioritize investments and minimize cybersecurity risk.

Start with the Business – the first stage of the assessment is to develop an understanding of the most business-critical processes, as perceived by organizational leadership and regulators. In most cases this is a relatively short step in consultation with business leaders. These processes are usually well understood, and the necessary process maps and descriptions will be available from previous work. A limited validation exercise is required to confirm that documentation provided is accurate and up-to-date.

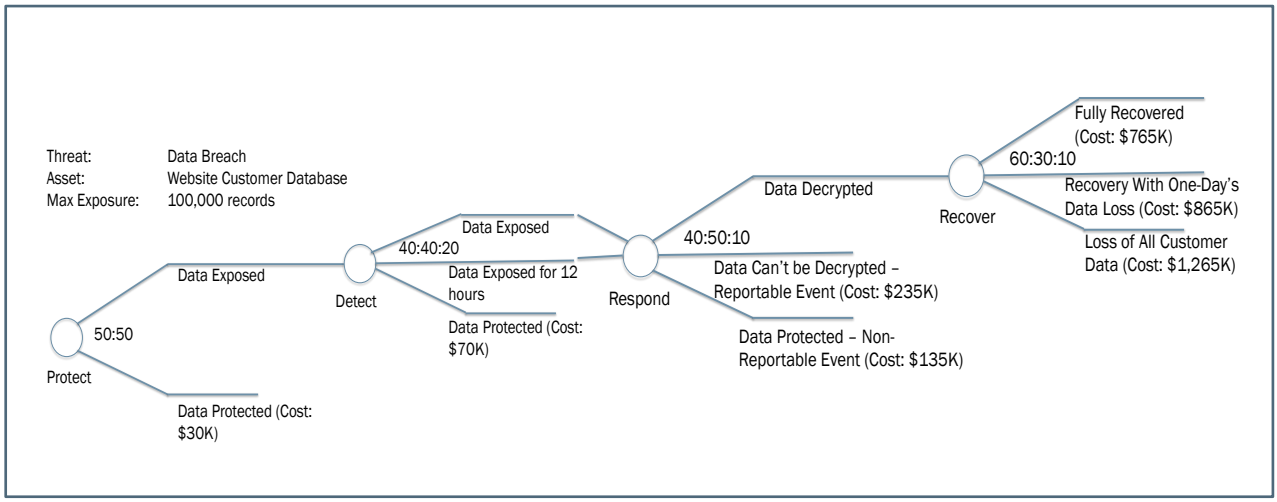
Understand the Most Critical Threats to the Organization – Cybersecurity threats come in many different forms and via multiple vectors, but the highest risks to an organization depend on its business – for example, a financial broker that makes high-value commercial trades in milliseconds has different business-critical risks to a retail bank that manages checking accounts for millions of customers. Bad actors understand these differences and

will marshal their attacks accordingly. A workshop with business leaders is used to prioritize threats.

Identify Critical Assets – It's important to understand the assets that support business-critical processes. Often these are process-specific assets, such as an application or database. General infrastructure assets such as email filters, access control systems, and firewalls shouldn't be neglected because of the ways that they protect the human interactions in the process. This stage of the assessment is investigative, and often relies on existing documentation, such as asset inventories and architecture diagrams, supplemented with one-on-one interviews.

Understand Asset Protection – This exercise is the core of the assessment. The cybersecurity protections at an asset level need to be understood, including an evaluation of the probability of them being overcome, and what remediation activities would be required. The information is gathered in a series of workshops with the staff who operate critical systems and protections.

Assess Scenarios – Finally, the asset protection models generated above are evaluated to prioritize the critical asset-threat combinations that may occur using a standardized "expected cost per incident". The prioritization is used to identify areas of improvement and can also inform cost-benefit analysis of improvement options.



Sample Critical Asset Protection Model

BENEFITS

Satori's scenario-based cybersecurity assessment augments traditional assessments through in-depth analysis of business processes, identifying the highest impact risks to applications and infrastructure. Result are used to prioritize investments and minimize cybersecurity risk.

Most organizations already have the core cybersecurity control set in place, but high impact failures continue to occur.

There are numerous 'shiny objects' available that aim to improve cybersecurity, but it is costly and complex to implement them all.

Satori's scenario-based approach focuses on areas of highest risk for the organization. Our decision-support tools and sensitivity analysis enable informed decisions, aimed at reducing the highest risks first.

At Satori Consulting, our mission is simple—to work side-by-side with clients to discover opportunities and solve problems. We strive to provide both comprehensive and expert service, mindful of every client's unique needs. Our team of highly-skilled management consultants brings a wealth of industry and functional experience to provide wide-ranging services in risk management, strategy and advisory, business process engineering, project and program management, change management, organizational effectiveness, performance management, and infrastructure and technology. We are not a reseller and consequently can provide object advice to clients.

48 Wall Street
Suite 1100
New York, NY 10005
Phone 212.918.4560

info@satoriconsulting.com