PSCU

PERSPECTIVES

Data is the New Cash for Criminals: ERM is the Best Defense

February 2016

Risks and threats to the economic health and brand reputation of an organization are everywhere. This is especially true for companies engaged in financial services – issuers, retailers, processors and other entities that conduct business in the payments industry. The job of protecting the organization and identifying risk today falls to a comprehensive and integrated Enterprise Risk Management (ERM) practice capable of adapting nimbly to the dynamic nature of the risk landscape.

There is the obvious and everyday threat to our most precious possession – our data. Financial institutions and their partners are arguably the most appealing targets for today's thieves and robbers. The new digital pirates invade with their keyboards and code. They find soft spots and target the vulnerable. They don't want cash outright necessarily – their bounty is your data. The 2016 version of a big heist might well be a tiny piece of malware. Or a worm that cyber criminals and fraudsters dispatch to burrow into a vulnerable system and score an outlaw's treasure of confidential information, which can be misused and spent many times over.

Rini Fredette
SVP Enterprise Risk Officer, PSCU

As Senior Vice President and Enterprise Risk Officer, Rini Fredette, provides the overall leadership, vision, and direction for assessing, analyzing and holistically managing risk across PSCU's organization. Rini leads the company's initiatives to develop processes that effectively manage risk within PSCU's tolerance thresholds and that tightly align with PSCU's strategic objectives. Rini's primary responsibilities include Enterprise Risk Management, Internal Audit, Vendor Management, Compliance Governance, Business Continuity & Life Safety, and Investigations & Corporate Fraud.

Or risk may be present in flawed processes eroding brand reputation from a failure to meet service level standards or falling short on a contractual promise.

Data is the New Cash for Criminals: ERM is the Best Defense

It's a Hazardous Life in the Payments Fast Lane.

Fortunately, for many organizations, Enterprise Risk Management (ERM) is getting the focus and support needed to protect an organization's most important assets – its data, its people and its brand reputation.

ERM is an umbrella term for the policies, processes and tools a company employs to identify and mitigate the main threats to the ongoing success of its business. The principles of how to implement ERM are similar from one company to the next but can vary depending on the particular industry. Here are three concepts to consider when shaping an approach to ERM:

Assemble an Integrated Team with Empowered Risk Champions

At its core, ERM is a proactive program with processes in place to identify risks of threats from internal and external sources, which could include employees, vendors, processes with control gaps and, of course, cyber-attackers with bad intentions.

Your ERM strategy should be organized and governed according to these three lines of defense:

Operational Management, which addresses risks to your company's operations and sources of revenue by ensuring effective internal controls. A significant risk component here is the technology and protocols in place to guard your company's (and your clients') data from cyber-attacks. Managing risk at the first line of defense requires a team of "risk champions" who are mid-level leaders and subject matter experts throughout an organization, including but not limited to IT, finance and accounting, sales and account management, operations, product management and your legal department. These advocates are empowered with identifying current and emerging risks and their priority levels throughout the organization, reporting risks into a centralized risk register, and enforcing the departmental policies in place to mitigate risks.

Risk Management, **Compliance & Oversight**, which involves the executive leadership team and risk committees to ensure the overall integrity of how well the company addresses various risks holistically across the organization in proper proportion to its strategic objectives and appetite for risk. A strong ERM team – which often includes functions for ERM, fraud investigations, business continuity, vendor governance and regulatory compliance – benefits the company through its ability to leverage and share information. This open awareness and free exchange of knowledge among team members work to expose issues, vulnerabilities in processes, or new potential and emerging risks across the entire taxonomy of corporate risk.

PSCU Forward.

Risk Assurance, which leverages Internal Audit to provide senior management with comprehensive assurance from an independent perspective. Internal Audit provides assurance of the effectiveness of governance, risk management and internal controls.

Spread the 'R' Word Through the Company

When ERM is woven into the fabric of a company's culture, everyone is a risk manager. The identification of risks and threats and how to properly mitigate them is the province of the many rather than the few. An internal campaign that urges employees to "say something" when they "see something" can be remarkably effective in bringing to light the dark side of risk. Companies that conduct and, in fact, mandate security and risk awareness training for all employees stand to fare well when it comes to lowering potential risk in all areas of their operations.

Look Beyond Your Own Walls

There's a new sheriff in town, and Vendor Management wears the badge. The complex nature of business in financial services, for example, brings a host of different players to a company's doorstep. Out of necessity, a company may need to partner with third-party service providers – such as software development firms or secondary solution firms – to implement its strategies and meet deadlines for certain high priority deliverables. A strong vendor governance program, backed by the support of the board and executive team, protects the company by insisting that vendors and partners demonstrate how they fortify their systems from intrusions and breaches that might also impact the company that pays them. Onsite vendor audits help verify that your vendor is not an indirect weak link in your threat mitigation plan.

Risk never sleeps, and it is everywhere. The benefits of an experienced and empowered ERM practice are immense and carry through to all parts of the organization. A more risk-informed company is better able to protect itself. The collection and analysis of a company's risk data keeps it aware of potential hazards now and in the future.

ERM is an investment in the ongoing security of the company, its people and its reputation.