TX Office: (817) 416-6842
NV Office: (702) 565-2727

Kral Ussery LLC
Certified Public Accountants
Advisors - Litigation Support - Internal Audit

February 20, 2020

The Importance of a Cybersecurity Strategy

Critical considerations for cyber readiness

By Ron Kral, CPA, CMA, CGMA
Partner, Kral Ussery LLC

No topic has likely garnered more attention in boardrooms over the last couple of years than cybersecurity. And rightfully so when the full extent of direct and indirect costs of a data breach are considered. Direct costs include legal fees, forensic experts, public relations, remediation efforts, potential fines and regulatory compliance expenses. However, it is the indirect costs of operational disruption, increased insurance premiums, brand reputational damage, loss of future revenue streams, etc. that can lead to business ruin. There is no shortage of specific cost estimates and articles on this important topic, and one research study pegs the total average cost of a data breach at $3.92 million.[1] Considering what is at stake, is your organization truly prepared to address cyber risks? This article offers some practical considerations to enhance cybersecurity.

The risk of a cyber incident, defined as a cyber security event that puts sensitive data at risk and requires action to protect associated assets, applies to all industries and companies of all sizes. No company is too big or too small, and smaller organizations tend to have higher costs relative to their size thus hampering their ability to financially recover from the incident.[2] However, it tends to be the larger ones that dominate press coverage and the lessons-learned can be insightful. For example, the table below highlights five notorious cyber incidents and their respective causes.

Organization & Year of Breach	Impact	Cause
Equifax - 2017	145 -150 million people	Failure to patch one of its Internet servers against a pervasive software flaw.
Verizon - 2017	6 million customers	Contractor failed to secure a large batch of customer information.

[1] Page 5 of Cost of a Data Breach Report 2019, research conducted by Ponemon Institute LLC, published by IBM Security.

[2] *We found significant variation in total data breach costs by organizational size. The total cost for the largest organizations (more than 25,000 employees) averaged $5.11 million, which is $204 per employee. Smaller organizations with between 500 and 1,000 employees had an average cost of $2.65 million, or $3,533 per employee.* Research conducted by Ponemon Institute LLC as published by IBM Security in Cost of a Data Breach Report 2019, page 7.

Boeing - 2017	36 thousand employees	Employee data left control of the company when a worker emailed a spreadsheet to a significant other.
Target - 2013	70 million customers	Hackers gained access to Target's POS systems using login credentials belonging to an HVAC company.
Yahoo - 2013	3 billion users	The hack came from a single user in Yahoo's corporate office. An employee was sent a spear-phishing email with a link, which as soon as they clicked on it, it downloaded malware on the network.

Examining the causes for these five high-profile breaches draws attention to the risks associated with;

- not understanding vulnerabilities nor taking timely action to address them,
- lack of vendor oversight and
- lack of employee education.

There is no shortage of security and IT control frameworks to help formulate a cybersecurity strategy. One of the more prominent cybersecurity frameworks is the NIST Cybersecurity Framework (CSF) published by the US government. The NIST CSF consists of five concurrent and continuous functions:

- **Identify** cybersecurity risk to systems, assets, data and capabilities
- **Protect** the organization from identified risks through controls to limit or contain the impact of a potential cybersecurity event
- **Detect** potential cybersecurity events in a timely manner[3]
- **Respond** to cybersecurity events, including having a response plan and performing activities to eradicate the incident and incorporate lessons learned into new strategies
- **Recover** from cybersecurity events through actions to restore impaired capabilities or services

At a minimum, all organizations should have these five functions addressed in a formal cybersecurity strategy document, sometimes referred to as a cybersecurity risk management program (CRMP). Many frameworks can be daunting in terms of their terminology and complexities as it is easy to get lost in the details. Here are some considerations in developing and deploying a cybersecurity strategy:

1. Utilize common language that is accessible and can be understood by all employees and relevant vendors.
2. Don't fall into the mindset that outsourcing to the cloud (i.e., electronic outsourcing) relieves management and the board from their accountability and oversight. While you can outsource the controls and process elements; the objectives, risks and ultimate control oversight resides with the procuring organization.

[3] *The average time to identify a breach in 2019 was 206 days and the average time to contain a breach was 73 days, for a total of 279 days.* Research conducted by Ponemon Institute LLC as published by IBM Security in Cost of a Data Breach Report 2019, page 6.

3. Formalize cybersecurity objectives, risk considerations and associated processes in writing through a CRMP. The AICPA's *Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program* is a great place to start.
4. Leverage control criteria to evaluate the suitability of design and operating effectiveness of controls pertaining to a CRMP. The AICPA's *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* forwards robust control criteria that utilizes COSO's 2013 *Internal Control – Integrated Framework*. The COSO *Internal Control – Integrated Framework* is widely used by US public companies and other organizations thus reducing the learning curve time of this control criteria.
5. Keep a sharp focus on the process and people (i.e., control owners) as these elements can matter more than the technology. A strong IT infrastructure will not be successful without healthy control processes and competent people.
6. Understand that the CRMP must be a living document that is continuously updated to address evolving risks. Cyber criminals are always trying to stay a step ahead of legitimate businesses thus posing new risks.
7. Assign a clear governance role at the board level to provide oversight of management's CRMP.

Remember that cyber readiness, including implementing a robust CRMP, does not happen overnight. It will take time and resources to build and maintain, but an important objective is to strive for continuous improvement to address changing risk landscapes.

Do not procrastinate when it comes to cybersecurity as the risks are real. While a goal of developing a CRMP leveraging security and IT control framework(s) should be of interest for all organizations, initial steps can be difficult. It begins with education and acquiring the expertise to assess the current state of cybersecurity objectives, risks and controls. An independent perspective can be an efficient and effective route for evaluating the current landscape. In addition, establishing roles and accountabilities at both the board and management levels is an important early step. Finally, for organizations with cloud computing, vendor management control also needs to be an early focus.

In conclusion, we must remember that hope is not a strategy. Cyber-attacks and data breaches are rapidly growing with greater sophistication. It is likely a matter of time before your organization is thrust into a serious cyber incident and if you have already been subject to one, be prepared for another. Don't be caught off guard as an entity-wide CRMP is essential in protecting shareholder value. A strong cybersecurity posture allows organizations to be more creative and proactive in the never-ending search of strengthening revenue streams and profitability.

*****

Ron Kral is a partner of Kral Ussery LLC, a public accounting firm delivering advisory services, litigation support and internal audits. Ron is a highly rated speaker, trainer and advisor. He is a member of 4 of the 5 COSO sponsoring organizations; the AICPA, FEI, IIA, and IMA. Contact Ron at Rkral@KralUssery.com or www.linkedin.com/in/ronkral.

Kral Ussery LLC serves US public and private companies to protect and grow shareholder value, as well as non-profits and governments with internal controls and in combating fraud. We assist entities with governance and in all matters relating to financial reporting, including SEC compliance, internal controls testing and remediation, IT general controls, IPO readiness, M&A transactions, and US GAAP. Visit us at www.KralUssery.com.

This is an article from the Governance Issues™ Newsletter, Volume 2020, Number 1, published on February 20, 2020 by Kral Ussery LLC.