Employing a Multi-Faceted Approach to Enhance Your Cyber and Data Security Plan for Small, Medium, and Franchised Businesses

Written by: Audrey E. Randall

January 29, 2018

No one could have predicted the speed in which technology would evolve in today's business landscape. Increasing reliance on internet dependent services continues to provide tremendous opportunity for growth, while simultaneously increasing vulnerabilities and threatening the financial strength and reputation of many small, medium, and franchised businesses. Hackers and other bad actors have identified small enterprise as "low hanging fruit", easy to target and often lacking the personnel and key resources to fully implement an information security and data protection plan.

For small business owners, any cyber incident has potential to severely handicap critical operations, destroy its reputation, and shutter its doors. Statistically, 43% of small business owners will encounter some form of a cyber-attack. Sixty percent of those businesses will fail within six months. For franchised systems, this is especially concerning, as the success of the brand is dependent on its reputation, financial strength, and ability to deliver the "intellectual property" rights that are licensed to their franchisees via the "franchise agreement".

> STATISTICALLY, 43% OF SMALL BUSINESS OWNERS WILL ENCOUNTER SOME FORM OF A CYBER-ATTACK.

Regardless of size, industry, or complexity, every business small, medium, large, franchised or not, must apply basic risk management strategies to protect the organizations brand, assets, and financial position. Implementing a cyber risk management program is not an either/or it must be an extension of the organizations overall risk program.

The working definition of Traditional Risk Management (TRM) as defined by the National Alliance for Education and Research is "The process of protecting an organization's assets through exposure identification, exposure analysis, controlling exposures,

financing losses with external and internal funds, and the implementation and monitoring of the risk management process". This approach addresses hazard risks that may result in loss to the organization and which need to be included in the corporate insurance program. The very minimum acceptable level of due diligence for any organization is identification of its exposures. Knowledge pertaining to the likelihood and potential financial and operational impact a cyber risk could have on the organization is gained through the ***identification process***. Additionally, the process identifies potential gaps in the insurance coverage that could lead to law suits in which the defense costs may not be covered under the ***Duty to Defend*** clause of the liability policy. Resulting damage to the organizations reputation, the legal and regulatory costs associated with non-compliance and increased data breach costs very likely would put the organization into the 60% that are unable to recover following a cyber incident.

Today, more and more organizations are recognizing the competitive value a comprehensive risk management program affords. Instead of viewing risk as potential for loss only (pure risk) they see risk as a competitive advantage representing opportunity for gain (speculative risk) and are actively managing their risk through an Enterprise Risk Management (ERM) process. This approach addresses risk from a strategic, operational, financial, and hazard perspective and views risk as potential for gain and not just loss. The ERM approach uses a multi-faceted process, works across company silos, and involves a broad selection of key employees, first-line leaders, and outside providers, working together to create a sustainable cyber risk management program that builds morale, increases cross-departmental collaboration, encourages team work and provides a foundational platform for leadership development.

Completing the ERM process will provide the organization with information about the likelihood and resulting business impact a cyber incident could have. This information is needed to assess and define the organization's risk culture and its risk appetite. Risk Culture is the system of values and behaviors present in an organization that shapes risk decisions of management and employees. Risk Appetite is the amount and type of risk that an organization is willing to take to meet their strategic objectives. Understanding its risk culture and risk appetite allows the organization to treat its cyber risk as a strategic business risk and builds the foundation used to develop the Cyber and Data Security plan aka cyber risk management program.

> Completing the ERM process will provide the organization with information about the likelihood and resulting business impact a cyber incident could have.

Does your company need a Cyber and Data Security plan? The easy answer is yes. But if you want a definitive yes/no then ask yourself these five questions:

Do you . . .

1. Have Employees?
2. Store or collect your clients' confidential digital information?
3. Use mobile technology?
4. Accept credit cards or other forms of payments?
5. Have any outside vendors or partners?

Answering yes to any of the above questions signifies that your organization needs to implement a process to identify, assess, and manage its cyber exposures. The constant evolving type and number of bad actors looking to gain access to an organizations data and the responding legal and regulatory environment continues to place new compliance demands on business. The National Conference of State Legislatures lists 42 of our 50 states introducing bills or resolutions related to Cybersecurity. At a minimum, organizations need to identify the type of information collected, *who* collects it, and *how* it is collected and stored. In addition to yours and your clients confidential and proprietary information, your cyber risk program must take appropriate action to protect:

- PII – personally identifiable information
- PHI – protected health information
- PCI – payment card information

The National Institute of Standards and Technology identifies two approaches to managing cybersecurity:

1. Manage cybersecurity risk across the entire organization
2. Manage cybersecurity risk and its impact to the delivery of critical services within the organization

Regardless of the chosen approach, the overriding goal is to use best practices and risk management principles to improve cyber security and resilience in coordination with the organization's overall enterprise approach to risk management.

THE OVERRIDING GOAL IS TO USE BEST PRACTICES AND RISK MANAGEMENT PRINCIPLES TO IMPROVE CYBER SECURITY AND RESILIENCE IN COORDINATION WITH THE ORGANIZATION'S OVERALL ENTERPRISE APPROACH TO RISK MANAGEMENT.

Recognizing the need to improve the cyber security and resilience of our country, the Obama Administration created The Cybersecurity Enhancement Act of 2014 (CEA). The CEA required The National Institute of Standards and Technology (NIST) to create a voluntary framework that focuses on using business drivers to guide cyber security activities. The administration mandated that the framework be "flexible, repeatable, performance-based and cost-effective". The resulting cybersecurity framework provides standards, guidelines, and practices that when applied to people and policies, devices and networks, websites and data applications mitigates cyber threats, increases response time, and decreases the overall business impact a cyber incident will have on the organization while protecting individual privacy and civil liberties.

***Flexible, repeatable, performance-based, and cost-effective* –** to accomplish these directives NIST created a Cybersecurity Framework with three components:

The Framework Core – consists of five concurrent and continuous functions:

1. **Identify** – Develop an organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities
2. **Protect** – Develop and implement appropriate safeguards to ensure delivery of critical infrastructure services
3. **Detect** – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event
4. **Respond** – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident
5. **Recover** – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident

Framework Implementation Tiers – provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. The tiers range from Partial to Adaptive and provide guidance to help an organization move from reactive response to cyber incidents to an agile and risk-informed response

A Framework Profile – A representation of the outcomes that a particular system or organization has selected from the Framework Categories and subcategories.

Additional information and guidance can be found at https://www.nist.gov/cyberframework

The Cyber Security Framework created by the National Institute of Standards and Technology is not mandated by the State or Federal Government. It does however, provide a comprehensive road map to help business owners create a viable cyber risk management program should they choose to utilize the tools and resource recommendations that are provided.

Additionally, there are many free resources available outside of the Cybersecurity Framework created by NIST. A few of those links are listed below:

- Federal Communications Commission: https://www.fcc.gov/cyberplanner
- Insurance Institute for Business & Home Safety http://disastersafety.org/ibhs-business-protection/ofb-ez-business-continuity

Insurance carriers and their agents are another great resource:

- Travelers: https://www.travelers.com/travelers-institute/cyber/symposia-series/hartford-ct-march-22-2017.aspx
- Hartford: https://www.thehartford.com/resources/cyber-liability-coverage-insights-expertise

Conclusion: Cyber threats have become ubiquitous across our business landscape. Cyber criminals are increasingly finding new and inexpensive ways to access an organizations computer network. In 2017, high profile cyber events like the Petya and WannaCry attacks moved ransomware from an unknown word into every day conversations. New and updated regulations about how you use, collect, process, maintain and discard personal information are constantly being evaluated. Sixty-six percent of our businesses are dependent on the internet to sustain and grow their operations. Technology continues to evolve and create new ways for us to store data and connect with each other creating more vulnerabilities and increasing the impact a cyber incident could have on an organization.

To stay viable and to protect its assets, financial position, and reputation, organizations need to develop a risk management strategy to address their cyber threats. By involving employees, third party partners, and other stakeholders small, medium, and franchised businesses can create a sustainable cyber risk management program that is affordable, facilitates team work and collaborations, builds brand name recognition, and provides a foundational platform for identifying high-potential employees and franchisees for leadership development and or expansion opportunities.

Audrey Randall is the President of Paradigm Franchise Group. Paradigm Franchise Group is a Franchise, Business, and Risk Management consulting firm dedicated to empowering entrepreneurs by helping to Start, Grow, and Protect small, medium, and franchised businesses.