Is Your Small Business Vulnerable to a Cyber Attack?

Albert J. Marcella Jr., Ph.D., CISA, CISM

Almost half of all cyber attacks, 43%, are directed at small businesses, according to data compiled by SCORE.[1]

When asked what information cyber attackers are most likely to target, 63 percent of respondents to the Ponemon Institute's 2017 survey, State of Cybersecurity in Small and Medium-sized Businesses, stated that customer records are their biggest concern. Possibly because this is the information smaller companies most often use. Almost half of respondents (48 percent) say they worry about the protection of their intellectual property.

Given that most businesses today operate in a 24/7, immediate access, information rich, global market space with users and customers seeking the same 24/7 access to these businesses and their products, it is safe to answer...data are one of an organization's most valuable asset!

But, which data? Not all data can be or should be treated equally. Some data are more sensitive than others. Some data retain their importance (value) for a longer period of time. While quite correctly, some data are important (or have value) for only a very short period of time before they become useless, public knowledge or no longer valid.

What steps can businesses take to identify risks that may directly impact their second most valuable asset? What questions should management be asking with respect to mitigating these risks?

The following five steps will guide your organization toward implementing a more proactive IT risk assessment process and to developing a stronger and safer cyber secure environment for protecting your organization's most essential data assets.

5 Proactive Steps to Help Your Business be more Secure against a Cyber Attack

Step #1 - Identify Data Assets

Some of the most important data to the continual survival of your business could be, but are not limited to, , personnel and client records, financial transactions, trade secrets, credit card information, PII/PHI, intellectual property, product designs, and forecasting models. In reality,

any data which your organization depends upon to continue day-to-day business activities and provides your business with a strategic advantage.

Questions management MUST have an answer to:[2]

1. Are established procedures in place and effective, in identifying and documenting the organization's most critical, sensitive, essential data assets?

2. Are employees subject to policies and procedures created to control their activities and to assure the protection of the organization's data assets?

3. Are contracted staff and other contract personnel subject to policies and procedures created to control their activities and to assure the protection of the organization's data assets including signing confidentiality agreements?

Step #2 - Classify Data Assets

Step #2 classifies data based upon their necessity and criticality to continue ongoing business operations and then associates them with an impact level.

Data asset classification:

- **Confidentialit**y - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

- **Integrity** - Guarding against improper modification or destruction of information including ensuring information destruction and authenticity.

- **Availability** - Ensuring timely and reliable access to and use of information.[3] Potential Impact Level - on organizational operations, organizational assets, or individuals:

- **LOW** if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect.

- **MODERATE** if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect.

- **HIGH** if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect.[4]

Questions management MUST have an answer to:

1. Has the business established a comprehensive data classification scheme, in accordance with the organization's security and privacy policies identifying:

- **Internal data** - data that should not go beyond the internal workings of the company;

- **Confidential data** - data that, if it were to be disclosed or released, without authorization, could cause the company severe financial, legal and/or reputational harm;

- **Regulated data** - data that is controlled by a state or federal regulation or other 3rd party agreement;

- **Public data** – data that can safely be shared outside the company?

2. Whom, within each user department is responsible for identifying and determining the sensitivity of data (e.g., data custodian, data owner), and this been communicated and have they accepted these responsibilities?

3. Has management defined, implemented and maintained security levels for each data classification?

Step #3 - Locate and Secure Data Assets

Data assets, once identified and classified, must be secured to prevent their unauthorized use, disclosure, modification, damage or loss. Proper data security will aid your business in protecting revenue, compiling with regulatory mandates, and generating/preserving brand loyalty.

Questions management MUST have an answer to:

1. Where are essential business data stored? Internally, externally, on user desktop machines, laptops, mobile devices? All of the above?

2. Who has access to these data?

3. Are all who have access authorized users?

Step #4 – Perform an Information Technology (IT) Risk Assessment

An IT risk assessment is the process of identifying risks to business operations including mission, functions, image, reputation, data assets and individuals, resulting from the organization's use of IT systems and applications. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place.

A threat is any circumstance or event with the potential to adversely impact business operations. A vulnerability is a weakness in an information system that could be exploited by a threat source.

Questions management MUST have an answer to:

1. Has your firm ever tested its network for vulnerabilities or performed a risk assessment?

2. Are adequate data protection procedures in place and monitored by management?

3. What is the expected impact from a single occurrence of a threat to your business operations?

Step #5 - Mitigate the Risks to Data Assets

Risk Mitigation involves the prioritizing, evaluating, and implementation of appropriate risk-reducing internal controls/countermeasures which provide assurance that technical systems operate as intended, provide reliable data, and comply with regulations.

Questions management MUST have an answer to:

1. Who has access to modify or delete data from its creation to disposal/archival?

2. How often is data protection awareness training provided and is there ongoing refresher training for staff?

3. Has each identified critical data asset been assigned an owner, a defined and agreed- upon security classification, and access restrictions that are periodically reviewed?

Managing risk is a complex, multifaceted activity that requires the involvement of all levels within the organization. Information technology (IT) risk assessments are fundamental to minimizing the consequences from a cyberattack.

Incorporating these five steps into a comprehensive, company-wide, risk management program, is essential in reducing your organization's overall cybersecurity risks.

Citations

1: "43% of Cyberattacks Target Small Businesses," (n.a.), (October 11, 2018), www.prnewswire.com/news- releases/43-of-cyberattacks-target-small-businesses-300729384.html

2 Note: The questions presented here and in the subsequent steps are provided as examples and represent only a small fraction of the questions that must be asked by management or by an information technology (IT) audit/IT risk management professional.

3: Federal Information Processing Standards (FIPS) Publication 199, "Standards for Security Categorization of Federal Information and Information Systems, 44 U.S.C., Sec. 3542," (February 2004), https://citadel- information.com/wp-content/uploads/2012/08/FIPS-PUB-199-final.pdf

4: Ibid.

ABOUT THE AUTHOR

Albert J. Marcella Jr., Ph.D., CISA, CISM
President, Business Automation Consultants

Dr. Marcella, President, Business Automation Consultants, (BAC) LLC, is an internationally recognized public speaker, researcher, and workshop and seminar leader with 38 years of experience in IT audit, risk management, IT security and assessing internal controls. Dr. Marcella, has authored numerous articles and 28 books on various IT, audit and security related subjects.

Article Citation

Marcella, A. (July 29, 2019), "Is Your Small Business Vulnerable to a Cyber Attack?" Service Corps of Retired Executives (SCORE) Greater Phoenix, https://greaterphoenix.score.org/blog/your-small-business-vulnerable-cyber-attack, 2828 N. Central Ave, Suite 800, Phoenix, AZ, 85004