Secureworks®

WHITE PAPER

The Value of Incident Response Planning

Are you protecting the business or simply securing the enterprise?

As an information security leader there is no “hard and fast” rule that defines whether or not you are doing a sufficient job.

However, once you have a breach, the expectations of your organization are clearly defined and backed by numerous regulators eager to show their constituencies that they mean business. This is a major concern for your senior leadership and is something you want to ensure you are prepared to deal with.

This white paper is intended to guide your incident response planning from a consequence management perspective, which will help you develop better incident response planning by:

- Addressing the strategic risk(s) of the organization
- Ensuring your plan is “actionable”
- Detailing a decision making process
- Making “your” plan an “our” plan
- Familiarizing and exercising your plan at least annually

While most organizations have threat and vulnerability management programs, very few, if any, have consequence management programs. However, consequences are the focus of the board.

Due Diligence

It was not that long ago that the primary challenge for information security leaders was getting the attention of corporate leadership. Their budgets were sparse, concerns anchored towards the bottom of the “corporate goals” list, and they were looked at as overhead. Well, today there is good news. Information security is now a board-level concern. The bad news: information security is now a board-level concern. Board-level expectations of the CISO/CSO may be requiring more than most are prepared for.

The concerns are justified; the number of breaches and their severity are increasing every year. While regulations are advancing around the globe, you only need to look at GDPR to see where the expectations on organizations are heading. Also look at the number of countries who have introduced or changed legislation, Hong Kong, Singapore, China, Japan, the Middle East, and Australia to name a few. The board cares about these because these are serious risks to the organization. Some might argue, depending on the nature of what you do or the depth of your coffers, that any one of these risks can result in a “business extinction” event.

There is another problem for CISOs; technology is not solving the problem. Threat actors buy the same technology you do, and they figure out how to beat it. Rather than focusing solely on preventing these events within your organization, you need to ensure that you have done due your diligence in planning to be able to detect and effectively respond.

Information security is a board-level concern for three major reasons: public interest in large-scale Payment Card Industry (PCI) and personally identifiable information (PII) breaches, breach notification legislation and litigation, and the rampant theft of intellectual property.

It Is All About the Business Risk

Risk = a Vulnerability that is exploited by a Threat, which manifests into a Consequence.[1]

As an information security leader, the technical aspects of your role are challenging and integral to the security organization. However, your understanding of the business and risks that threaten the ability to do business requires understanding security from a business consequence management perspective.

While most organizations have threat and vulnerability management programs; very few, if any, have consequence management programs. However, consequences are the focus of the board.

Today, the consequences of a data breach only continue to grow. Add to that the myriad of various regulatory and contractual obligations, and it only gets worse. The truth is that up until you are breached, the standards of due care are still fairly nebulous.

As an information security leader you are expected to do the best you can with the resources you have. There is no "hard and fast" rule that defines whether or not you are doing a sufficient job. However, once you have a breach, the expectations of your organization are clearly defined and backed by numerous regulators eager to show their constituencies that they mean business.

This is what your board fears most and is probably the last thing you are prepared to deal with.

Granted, there are standards such as PCI and ISO 27K but, in reality, there are costs and resource limitations as you compete with other business risks and demands.

The Value of Incident Response Planning

Think of Incident Response Planning as "documented due diligence". Additionally you have to steer your thinking from the plan being "yours". It needs to be an "our" plan. The thorough plan will require you to get out of the comforts of IT and expand professional relationships with folks in Legal, Treasury, Public Affairs, Corporate Risk Management, Investor Relations, HR, Fraud, just to name a few. The key is creating those relationships with parts of the organization that are stakeholders in the business implications of a cybersecurity event. This is about addressing the consequence component of business risk when your Prevention and Threat & Vulnerability (TVM) efforts have failed.

How Do I Know if I Have a Good Incident Response Plan?

There is no one "right plan". Each plan is unique to the organization that it serves. But here are a number of thoughts you should consider, either about the plan you currently have, or the plan you probably should have:

[1] U.S. Department of Homeland Security

Think of incident response planning as "documented due diligence".

1. **You are addressing the strategic risk(s) of the corporation.**

   You should be involving every possible resource available to deal with this problem. Your solution needs to be a "business solution" not an IT solution. That means resources outside of IT and outside of the company; Legal, PR, HR, and so on. If you aren't sure what the strategic risks are for your publicly traded company, look at the Cyber Risk(s) statement in your company's Annual Report (SEC 10-K). This is what the Board of Directors has identified to the owners of the company what their Cyber Risks are.

2. **Your plan is "actionable".**

   Do you have, BY NAME, resources to handle items such as credit monitoring, mail notification, forensics, and so on? Actionable information for these organizations can include cost, who to call and what information they will require. Maybe even have their contracts reviewed ahead of time so that there is one less thing you have to deal with when the alligators are gnawing at your toes.

   Work out as many of the templates as you can. Notification letters, acquiring bank forms, named points of contact. GDPR requires that organizations give notification within 72 hours, so being ready when the time comes is critically important.

   If some of this is just "too much effort", then leave it for your first Tabletop test and make that part of your scenario (just keep the results and add them to your plan later). In time of crisis you don't want to be running these details down. You're going to be busy enough with all the stuff you couldn't/didn't anticipate. The last thing you want to be saying to yourself is "Would'a, should'a, could'a"…. (It's also the last thing you want your management/board thinking to themselves.)

3. **Your plan details a decision-making process.**

   There is one thing worse than bad decisions during a crisis: it's not making decisions. Is it a person, or a committee? Do you already have a Corporate Crisis Management Team? If so, integrate them into the plan. Does the CISO really have the authority to make a business impacting decision? Don't wait until you are in the middle of a major crisis to figure out that everyone has an opinion, but nobody really has the authority to take action.

4. **Making "your" plan an "our" plan.**

   Your plan has been socialized with all of the participants and stakeholders, and their feedback has been incorporated. It can be tedious and challenging to de-conflict all of the differing perspectives and opinions, but at the end of the process you have a documented plan that everyone has had a chance to contribute to and implicitly approve.

5. **Your plan has been tested at least annually.**

   Never mind that regular testing is a requirement of every framework out there. Getting all the players around the table for a "Tabletop Exercise" is a great way to continue organizational visibility into the plan and to validate that the decisionmaking process still works. Most importantly, validate that your plan is still on track to solve the problem and that the problem has not changed since you last wrote/updated the plan. Maybe even make some friends outside of IT.

6. **If your plan cannot be used to address a lost file cabinet of personnel records (PII), then you need to rethink your plan.**

   The vast majority of breaches today around PII and PHI are due to complacency. The government still expects you to treat these breaches the same.

7. **Your Cyber Insurance Policy is integrated within your CIRP.**

   At a minimum, make sure the Cyber Insurance manager is a member of the CIRT. Your company is paying for that policy to mitigate significant financial risks. Failure to comply with its provisions may jeopardize your ability to get reimbursed. These stipulations typically apply to preferred vendors and notification obligations.

Conclusion

Sound information security management principles suggest that all organizations entrusted to maintain the confidentiality, integrity and availability of sensitive data should incorporate protective, detective and corrective measures to ensure such a result. Incident response planning is a corrective mechanism and should be part of any information security effort. For planning to be an effective corrective mechanism, it must provide a solid foundation as to its execution, specific information so that participants are empowered with current and relevant knowledge, and yet be broad as to not constrict an organization's ability to respond to unforeseen events. A plan's true value is measured by the relevance of the information and processes it provides at a time of crisis.

Planning will rarely answer all the questions that come up during an incident, but it should provide a repository of thoughtful anticipation, collaboration and research. Furthermore, to assure a plan's continued usefulness, it should be tested and updated on a regular basis.

Additional Resources:
https://www.nacdonline.org/Resources/Article.cfm?ItemNumber=7024
http://www.protiviti.com/en-US/Documents/Surveys/NC-State-Protiviti-Survey-Top-Risks-2015.pdf

Secureworks®

Secureworks® (NASDAQ: SCWX) is a global cybersecurity leader that protects customer progress with Secureworks® Taegis™, a cloud-native security analytics platform built on 20+ years of real-world threat intelligence and research, improving customers' ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

Corporate Headquarters

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp