WHITE PAPER

GILLIAM SECURITY

Where to Start When Starting with Security

Today is day zero in your organization for building security, here are the first steps.

Security can be intimidating at first. The words "I feel like the sky is falling, just tell me where we need to start" are often said.

One of the goals of the security program should be to have a positive employee experience that makes an impact on the organization to disrupt your industry with using security as a competitive advantage resulting in the insurance of additional revenue for years to come!

That said, how does one start? Let's jump in!

Step 1: Understand what and who you have at your fingertips.

To first understand where the organization can start with security, it needs to be understood what the organization has done for security previously. It is rare that nothing has been done as there is a good chance you will find breadcrumbs scattered, whether it be the running of Microsoft Defender weekly to changing all passwords on the "routers" bought from Best Buy when the company started.

Typically, these breadcrumbs will include things such as:

- Persons that have taken on some capacity to help in security;
- Software licenses from tools such as McAfee, Symantec, Kaspersky Labs, etc.;
- Reports from auditors or investors detailing some kind of security analysis;
- Data on financials surrounding previous spend for IT or security tools; and,
- Metrics that may give light to certain activities taking place and how often.

As part of this understanding is completing a risk assessment. You risk assessment should include at least the following:

- Governance of the business and documentation, to include policies, procedures and standards;
- Business, IT and logical architecture for the key critical business applications;
- Legal and regulatory requirements that govern the organization; and,
- Operational business process that drives the organization.

Step 2: Start building relationships and find a mentor within the organization.

Security is a difficult topic for anyone as it usually is not pretty. To help with the delivery of the message, establish relationships and a mentor in the organization so you can work with others in the organization to both craft your message and understand who key players are in the organization.

Step 3: Prepare to talk Board-level Information Security to business leaders.

At the VP-layer outside of IT and Information Security, one is not going to understand a presentation on the use of deprecated TLS on a load balancer. It may even be likely if security resources are existing in an organization, they may not even approach security from a technical lens so they may not even understand it.

That said, prepare to speak from the business perspective. Some of the key things to focus on when speaking to an executive include:

- *Focus on the quantitative data.* TLS may be critical but it won't sell as much as "the use of poor encryption exposes our organization to $25 Million of security risk." You may ask, "Where did the $25 Million come from?" Take your total records exposed by the use of your deprecated TLS and multiply the count times the average cost per record for the year from Ponemon Institute (link).

- *Focus on how it relates to the business strategy.* If the organization plans to expand into organizations where GDPR is enforced and you have no compliance program to GDPR, using the first bullet point, explain the compliance risk as it pertains to the business strategy. In this example, an organization can be fined up to 2 Percent of revenue (link).

- *Document your desired result and work backwards.* A meeting with a business leader or investor may be 30 minutes at best so it is important to understand what the result of the meeting should be prior to meeting. Once the goal has been outlined, outline the steps to achieve that goal so by the end of the meeting actionable results and next steps are available.

Step 4: Have answers ready to common questions surrounding your program.

Whether it be in a meeting or via a quick message on Microsoft Teams, common questions across all verticals exist that one should be prepared to answer. These include:

- Do we have a plan if we get hit with a ransomware attack?
- Where is our policy on *x* and what do I need to do get it approved?
- Are we able to transfer the risk of *y* to the cloud or a third party?
- We have a contract stating to be compliant with *z*, are we good to sign it?

Have each of these questions ready with an answer that you can speak to.

Step 5: Begin building the fundamentals to your security awareness program.

As you build out your program, begin drafting a security awareness program, as this will help evangelize the program you are building to others. While it will not be your final program, it will help promote your program.

Seem intimidating to have all of these steps to do? Contact us and we can help you find and provide these answers based on our experiences at multiple organizations.

Why Gilliam Security?

Gilliam Security has recognized consultants from major fortune 500 companies with certifications such as the CISSP, CISM, CISA and CRSIC. Each consultant also has experience in building the information security, as well as privacy, function from inception to maintaining operations.

Contact Us Today at sales@gilliamsecurity.com