How a Strong Cyber Security Posture Creates Efficiencies in the Selling Process

Contents

SECURICY

Executive Summary

Your cyber security posture could make or break contracts with large organizations and governments. The cost of cyber crime to these entities has accelerated in the past five years. Malicious insiders cost companies the most per breach due to the lengthy time it takes to be resolved. For this reason, large companies require SMEs to have a strong cyber security posture or become compliant with an international standard.

The simplest way to increase the strength of your cyber security posture is creating and implementing a diligent cyber security policy. This step usually involves consultants that charge a hefty premium by the hour. Securicy offers you a fast, simple, and affordable solution. The Policy Builder platform instantly delivers a customized cyber security policy that makes your company compliant with your industry's standards. We also include a virtual consultant session with the policy builder to fully assess your current stance and guide you through the platform.

Securicy is a cloud-based platform that provides organizations the tools they need to quickly and efficiently get a cyber security strategy in place, build a human firewall, and step-up their overall cyber security plan. To learn more about our solutions, visit our website www.securicy.com and get started instantly. We are very passionate about reducing cyber breaches and regularly publish tips on improving your organization's security on our blog.

The Evolution of Cyber Crimes

The average cost of crime has been increasing every year as seen in Figure (A). In 2017, large corporations with over 1000 employees on average incurred $11.7 million in cyber-crime costs, a 22.7% increase over the prior year. Figure (B) breaks down the average cost of crime to industries with financial services being the highest due to the highly valuable personally identifiable information they store on customers. The yearly increase in cyber crime costs has been driven by the increase in the average number of security breaches per year. Large enterprises now face, on average, one security breach every three days.

Figure A

Figure B

The Cost of Malicious Insiders & Code

Malicious code and malicious insiders cost large companies $1.28 and $1.56 million, respectively, every year. It takes organizations more than 50 days, on average, to recover from these attacks. This makes each malicious insider or malicious code breaches cost more than $100,000 individually. This category of threat could come from any person or entity with access to the company's assets or data. Large companies mitigate this risk by ensuring third party companies that have access to any form of their assets are compliant with international cyber security standards. Regardless of the type of attack, when a publicly traded company announces a data breach, on average its stock price falls by 5% and they do all they can to prevent it.

Why do Companies Require Protection From SMEs?

Customers have high expectations from companies to securely store their data. In fact, 71% of consumers believe organizations have an obligation to control access to their information. Cyber breaches not only affect enterprises by incurring unexpected costs, they tarnish a brand's image. When a company is breached customers start questioning the integrity of their data. In the USA, 1 in 5 banking customers will switch to another bank if their account became compromised or their bank was breached. In the UK, customers are 30% more likely to switch to a competitor if a company they transacted with got breached. Globally, customer retention is being challenged in the active environment of cyber breaches.

The various costs associated with cyber crimes have led large corporations and governments to adopt strict cyber security postures. When these entities engage in any form of business with new parties, they ensure that these agreements do not come with any loose ends. Enterprises are forcing smaller companies to adopt stringent cyber security policies and become compliant with international standards. Since business agreements can lead to malicious insiders or malicious code, the threat to a large corporation or government is significant. Becoming compliant with international cyber security standards will enhance a small-medium enterprise's (SME) sales process to larger corporations for governments.

A Poor Cyber Security Posture Damages Your Sales

Every SME that's selling or wants to sell products to larger companies or governments needs to enhance its cyber security posture to prevent any hiccups in the sales process. If your company is signing a contract with a large organization or government, they might ask you to become compliant with one of the following standards:

ISO/IEC 27001 **NIST 800-12** **GDPR**

Some SMEs have lost large opportunities that never came back because they were not compliant or ready to be compliant at the time of signing contracts. Marcato, a live events management software, elaborates on the extent of this issue:

When Marcato got the chance to work with Disney, it was an enormous opportunity for the small business. A small tech company from Canada, Marcato had spent 10 years building a strong reputation working with the biggest names in the music, food, and film festival industries.

Then the deal started to unravel.

When Marcato was in the middle of closing the Disney deal, the team at the Mouse House intensively scrutinized Marcato's cyber security posture. After several conversations between the two companies, Marcato, led by Darren Gallop and Laird Wilton, went back to the drawing board in an attempt to become compliant with Disney's cyber security standards. But this process was lengthy, stressful, and costly. Eventually the deal fell through and Marcato suffered its biggest loss in company history.

The Benefits of Having a Strong Cyber Security Posture

Having a strong cyber security posture can enhance every business's sales process. For example, the United States Department of Defense will not award any contractor with a tender if their company is not NIST SP 800-171 compliant. On top of that, it is a contractor's responsibility to ensure that any subcontractors are also compliant. If your venture is in the Industrial Internet of Things industry, then most of your customers will require you to be ISA/IEC-62443 compliant. There are broader internationally recognized cyber security compliance standards that have become essential in most business deals. By becoming compliant with a cyber security standard, you ensure that your own company's data is better protected and prevent any hurdles in future sales.

Regardless of compliance, creating and implementing policies is an important step in enhancing your company's cyber security posture and mitigating the risk of successful data breaches. This leads to lower legal, marketing, and operating expenses. Your customers and business partners will trust you further with their data knowing that your company takes the security by design path. You can also use it as an opportunity to engage with your employees and instill the importance of cyber security threats to create a safer organization. Customers have high expectations from companies to securely store their data. In fact, 71% of consumers believe organizations have an obligation to control access to their information. Cyber breaches not only affect enterprises by incurring unexpected costs, they tarnish a brand's image.

SECURICY's Solution for Customized Policy Building & Compliance

Instead of spending the time and money it takes to hire a consultant to create policies for you, with Securicy it can be done in a matter of minutes. After answering a series of questions about your company, the Policy Builder platform will start generating the policies you need to be compliant with industry standards. You are able to review and download the policy, here is a sample policy:

Email Policy

Sample Policy

Purpose and Scope

The purpose of this policy is to define the usage of Sample Company email systems, whether managed by employees or by third parties. Every individual user who accesses Sample Company email systems must follow this policy.

Usage

All use of email must be consistent with Sample Company policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.

Sample Company email accounts should be used primarily for Sample Company business-related purposes; personal communication is permitted on a limited basis, but non-Sample Company related commercial uses are prohibited.

The Sample Company email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any Sample Company employee must report the matter to their manager immediately.

Users are prohibited from automatically forwarding Sample Company email to a third party email system. Individual messages which are forwarded by the user must not contain Sample Company confidential information.

Sample Company employees shall have no expectation of privacy in anything they store, send or receive on the company's email system.

User Responsibilities

All users must be aware of the means by which their computer may be compromised and be cautious when opening both emails and email attachments.

Users must know the type of file they are opening and should have their computer system configured to show all file types and extensions.

Users must not open email attachments that are suspicious and only open attachments when they know it was really sent by the person who is claimed.

Benefits of Using the Securicy Policy Builder

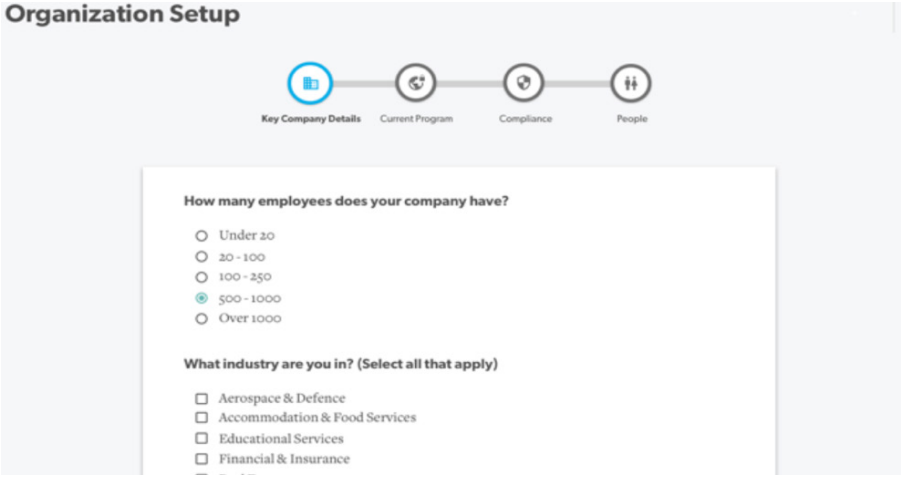
The Securicy Policy Builder enables you to efficiently build policies that are customized to your business and your industry, without breaking the bank. We know the process of creating policies is time consuming and could be challenging for those that don't have any expertise. Our platform asks you a few key questions to determine which policies best fit your company and you receive those policies instantly. The solution is fast, simple, and affordable! We provide the same services as consultants at the fraction of their costs. In addition, you receive access to our virtual consultants to have the peace of mind of an experienced professional and ensure you reach viable level of security.

Every purchase of policy builder includes a free 30-minute consultation with a certified security specialist. Our virtual consultant guides you through a streamlined process to easily build a customized Cyber Security Strategy that fits your organization. You get the services of consultants, without paying the premium!

Build a Strong Cyber Security Posture

A strong cyber security posture starts with a strong internal policy that clearly outlines the steps that need to be taken to become more secure. Please visit our website, www.securicy.com, to get started.

Setting up your policies is as easy as this:



"Our clients include NASA, GE and Lockheed Martin. To be an industry leader in our space we need to have strong Cyber Security Policies in place and regularly demonstrate that they are strictly followed. Securicy's platform enabled us to get our Cyber Policies in place and really makes it easy for us to prove to our clients that we take Cyber Security and their data seriously."

—**Dr. Douglas Milburn**, Co-Founder and Vice-President – Protocase