Why Cyber Security is a Necessity Rather Than Being a Luxury Cost

The way business is being conducted has changed immensely over the past two decades. However, it will continue to change as the rapid expansion of the Internet of Things, also known as IoT, is growing into more traditional industries. These are industries that previously lacked the necessary digital infrastructure needed to meet 21st-century requirements. The digital age offers companies and business owners access to new opportunities and innovations within seconds. This is something that previous generations could have only dreamed about having in their lives. After all, it enables them a greater opportunity to succeed, make a profit, and achieve greater ambitions.

However, opportunities of this magnitude do not come for free as they have great costs associated with them, which are mainly cybersecurity threats. The days of analog dominance are quickly coming to an end and are rapidly being replaced by digital codes that immediately revolutionize the strategies and cultures of numerous industries. It's important to note that these digital codes that cause all this great change has created new vulnerabilities that make companies and businesses more susceptible to being hacked by unknown cyber assailants. We found that 2017 was another heavy year for cyber attacks, security breaches, and theft of private information. From the Equifax privacy breach to the ongoing theft of data from U.S. government security clearance holders, the cyber infrastructure of government and commercial organizations must invest into integrating cybersecurity strategies as a permanent portion of their budgets.

According to a survey report by the PwC 2018 Global State of Information Security, 44% of 9,500 surveyed executives say they are aware of the growing concern of cyber threats. However, the 44% said they currently lack any kind of overall information security strategy. In addition, a 2017 Online Trust Alliance (OTA) report estimate that over 93% of security breaches can be easily avoidable by applying basic IT industry best practices that are widely adopted by the Intellection Group. This is why it is important for organizations of all sizes to know how important basic safeguards are needed to achieve at least a first line of defense. The OTA also considered 2017 as another "worst year ever" in the escalation of personal data breaches and cyber incidents such as data theft, ransomware takeovers, business email compromise (BEC) for financial or credential theft, and the infiltration of Internet of Things (IOT) connected devices.

Allocating a portion of an organizational budget to cybersecurity ensures that the organization is better equipped for any kind of cyber attack. In fact, it ensures business survival as 60% of small to medium-sized businesses (SMB) that are attacked end up going out of business within a year because they can't afford the costs of doing damage control. More alarmingly, small to medium-sized businesses are more likely to fall prey to cybercriminals, as they are their favorite and easier-to-reach targets.

As a result, organizations that are ill-prepared tend to find themselves being overwhelmed and in a very difficult hole to get out of. Four of the most common reasons why companies in this situation end up failing:

1. Lack of investment in adequately-sized IT departments to stay abreast of current threats to all the systems they are protecting;
2. No available protocol for ongoing cybersecurity training and education of employees in order to ensure they are up to date on the latest threats and safeguards;
3. Not possessing cyber insurance policies to cover the cost of dealing with ransomware attacks;
4. Inability to repair the public relations damage as a result of data theft, and lacking resources to conduct the proper damage control to contain the crisis.

These are weaknesses that no business of any size should have to endure in the digital age, and all are preventable or properly addressed with the right advance planning and preventative action. It's critically important to invest in IT services that will help detect, prepare, combat, and alleviate the risks caused by cyber-attacks and data theft.

Cybersecurity firms like the Intellection Group are here to assist the customer with a wide range of services that are preventive and ongoing maintenance-related. Instead of a business spending in-house IT resources to attempt learning and managing the ever-changing nuances of cybersecurity requirements, the Intellection Group can serve as an integrated resource while in-house teams concentrate on the business of doing business.

https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html

https://www.otalliance.org/system/files/files/initiative/documents/ota_cyber_incident_trends_report_jan2018.pdf

https://www.sec.gov/news/statement/cybersecurity-challenges-for-small-midsize-businesses.html

https://www.csoonline.com/article/3267715/cyber-attacks-espionage/4-main-reasons-why-smes-and-smbs-fail-after-a-major-cyberattack.html

https://www.techrepublic.com/article/2017-was-worst-year-ever-in-data-breaches-and-cyberattacks-thanks-to-ransomware/

https://www.forbes.com/sites/louiscolumbus/2017/12/10/2017-roundup-of-internet-of-things-forecasts/ - 2d9a50801480