The Dilemma of Medium and Small Businesses

In the Cyber Domain

Robert S. Powell, Jr.

Introduction / Summary

Medium and Small Businesses (MSBs) are faced with the same Cyber threats and requirements that large businesses are faced with. The large businesses are able to hire highly experienced cyber personnel to mitigate this risk to their survival in the business world. The MSBs face them with considerably lower budgets and inexperienced IT personnel. Although hardware and software solutions abound with the ability to counter the cyber threats, the lack of cyber experience of the MBSs' IT personnel make the utilization of these solutions weak, if not ineffective, in their environments. This paper will make the case that the lack of cyber experience by MSBs' IT personnel can be mitigated, if not eliminated, by cyber security knowledge. This knowledge can be gained by attending cyber security training conducted by instructors with cyber security experience in adverse and dynamic environments.

Background / Problems

Our world is changing at a rapid pace and the criminals are picking up speed. A few years ago all the security the local IT administrator had to focus on was system patches and ensuring that the Microsoft Exchange Server was running the current antivirus signatures. Those days are gone. We live in an era when data breeches are common and the compromise of customer accounts is at an all-time high.[i] Zero Day vulnerabilities run amuck and the hacker tools to exploit phones, PCs, tables, routers and switches developed by the US Government and foreign intelligence services[ii] are exposed to criminal hackers for free. In Oct 2018 30 Million Facebook accounts were hacked[iii] and Google+ had 500 thousand users' data exposed due to massive data breach[iv]. How long will your customers stay with you once they know that you were compromised and have exposed their data? If they take their business elsewhere how long will it take you to replace them? During the cleanup you may not have full access to your network. If you didn't have access to your customer data, accounting database, and your critical data in the network, how long could you stay in business?

To meet these challenges the large businesses normally hire a Chief Security Officer (CSO) with ten or more years of experience. An individual with this experience can cost a company from $100K to $164K to maintain on staff.[v] These individuals develop the cyber security strategy to protect the corporate assets of the company.[vi] They ensure the IT infrastructure meets the communication requirements while protecting employees, customers, partners and the company's reputation. They utilize their in-depth experience to integrate Cyber Security software, hardware and practices throughout the corporate environment. They are executive level personnel who execute cyber security policies and measures through cyber security engineers and IT staffs.

The IT staffs of MSBs are required to respond to the same vulnerabilities as the CSO with little to no cyber security experience to guide them. Their experience resides in ensuring that business components can communicate and remain available, not in protecting the communications. How can the MSBs mitigate the lack of cyber security experience on their IT Staffs without hiring a CSO and supporting CS Engineers?

Solution

Unlike large businesses, MSBs are highly adept at utilizing their available resources in order to maintain a competitive edge. Cyber security should be no exception to this rule. You could spend most if not all of your cyber security budget on hiring an expensive executive and a few cyber security engineers to work with your IT staff. This will not be an immediate fix due to the fact that these new personnel will need to learn the network and then gain a full understanding of your business process so that they can then develop the cyber security strategy to protect them. Do you already have individuals that fully understand the network and have an excellent understanding of what IT assets are used in the business process for you environment? Would your current IT staff not fit this criteria? Now you have identified that you have half of the solution in house, but how do you get them access to the knowledge that the more experienced cyber security individuals would have? You could look into cyber security certification training as a possible solution. Certification training is a good measure on how well an individual has grasped a specific block of instruction. But certification training is mostly focused on specific answers to specific questions that an individual can expect to see on the certification exam. The instructors are not focused on helping students apply the instruction to their environment. The US Army has struggled with these same issues. They sought a solution on how to bring new and current IT Soldiers up to a level where they would be effective when entering the actual cyber environment. Their solution was to utilize instructors with cyber security experience in highly dynamic military networks to provide the instruction. This instruction is conducted in a classroom type setting affording the students the ability to ask questions specific to their organizational environment. Courses cover more than would be expected at a certification boot camp. Certification is still utilized but instruction is based on the information expected of the student when they complete the course, not on what is expected to be on the certification exam. Individuals leaving these courses go back to their organizations not just with a new certification, but with actual knowledge of how to implement cyber security in their environment.

Advertisement

Succeed to Lead, LLC (STL) provides Cyber Security Instructors to 7 US Army Continental United States (CONUS) sites, as well as a Cyber Instructor Mobile Training Team (MTT) to support CONUS and overseas requirements. The primary site is part of the US Army Cyber Center of Excellence at Fort Gordon, GA.

We employ highly accredited staff, many of whom are former cyber security and IT specialists with the military, to provide top-to-bottom cyber-security protection. Our experts hold certifications such as CISSP (Certified Information Systems Security Professional) and CEH (Certified Ethical Hackers). They are thoroughly vetted and routinely trained on the latest technology, threats, and security methods.

We have extensive capabilities developing cyber security instruction and also training users on the use and application of cyber security tactics, techniques and procedure. We provide annual

cyber awareness training to military and government personnel. We also provide courses such as CompTIA Advanced Security Practitioner (CASP), Security +, Network +, Certified Information Security Manager (CISM), CyberSec First Responder (CFR), as well as customized courses to meet emerging requirements.

Many of our personnel are experienced in providing support to DoD Information Assurance Cyber Security validation teams. These teams are responsible for testing and certifying that the DoD networks are compliant with DIACAP, NIST SP 800-53, FISMA, and HIPAA regulations. As part of these teams they have developed detailed incident response plans/checklists as well as contingency plans, continuity of operations plans, and configuration management plans for multiple organizations. Our trained professionals stand ready to help prepare your IT staff to protect your company's assets from a cyber-attack.

Conclusion

The cyber world is changing at a rapid pace and the dangers for any size company grow every day. The need for cyber personnel with the required knowledge can no longer be ignored. Spending your limited budget to hire new personnel may not be fast enough, and it may not leave enough to purchase any new software or hardware needed to protect the environment. Training your current IT staff to fill these positions is faster and more economical. Succeed to Lead, LLC, has the capabilities to provide the level of cyber knowledge to get your IT staff past the initial certification stage to actually protecting your networks from cyber-attack. Don't wait until your network is at the mercy of the cybercriminal!

Works Cited

[i] https://www.bankinfosecurity.com/us-data-breaches-hit-all-time-high-a-10622
[ii] https://thehackernews.com/2018/03/nsa-hackers-tracking.html
[iii] https://thehackernews.com/2018/10/hack-facebook-account.html
[iv] https://thehackernews.com/2018/10/google-plus-shutdown.html
[v] http://www.payscale.com/research/US/Job=Chief_Security_Officer_(CSO)/Salary
[vi] http://work.chron.com/roles-responsibilities-chief-security-officer-19479.html