The Security Equals Compliance Disconnect

Cyber Security Summit Webinar Series
July 26th, 2022

Speaker: Jeff Hall, Principal Security Consultant, Truvantis

Moderator: Sean Costigan, Director & Co-Founder, ITL Security; Professor at George C. Marshall European Center for Security Studies

Report Author: Joseph Mathias, Executive Cyber Coordinator, Cyber Security Summit

Speaker Bio:
Jeff has over thirty years of experience in information technology, information security, and IT governance. He started his career as an IBM systems programmer writing and supporting operating systems, moved into application development, enterprise project management, CIO roles, CISO roles, and then started a multinational consulting firm's information security and PCI practices.

Jeff's expertise ranges from operating systems to networking, enterprise application suites, information security, and the cloud. He has been involved in a variety of projects to develop and implement innovative applications and services for small and midsized businesses to the Fortune 100. He has worked with manufacturing, distribution, financial institution, insurance, health care, and government organizations.

Introduction:
Security is an idea we generally have in the back of our minds; we are never focused on it until it is too late to do anything about it. This is a topic that no one really wants to talk about because they would have to admit that they aren't fully compliant with their security. The following Rapporteur discusses how risk assessments are generally outdated and how being compliant does mean an increase in security.

The Purpose of Risk Assessment
Throughout the years, people have attempted to create better security frameworks for their technology, leading to people performing risk assessments throughout their companies. These risk assessments aim to see if there are any security flaws in their hardware, systems, etc., and generally, there are. This is because the risk assessment they use is typically outdated or non-existent. Most organizations believe that to perform a good risk assessment they would have to have a complete department of employees focused on just that task. To make risk assessments more accessible, companies have started to use a divide and conquer strategy by using targeted risk assessments focused on specific processes or

departments. This means that every section of your company performs risk assessments, which are then all collected and united into an overall risk assessment. Even still, no risk assessment is perfect. You will have to have penetration testers, and you will have to cut down on the unnecessary individual risk assessments so as not to be overwhelmed with potential risks.

Compliance Does Equal Security

Compliance does equal security, but generally, this won't work because people are not compliant enough with the security measures. Most companies would average around 80%-90% compliance with their security which can lead to horrible consequences for the company and their customers. Another problem we face with security is that we tend to avoid it until we have a security issue. We need to integrate our security systems into our daily operations to catch these problems before they become too large for us to handle. This doesn't just mean that security is all up to the IT, but it's up to everyone in your company. If you want to keep your information and your customer's information safe, you need to have everyone in the company being compliant, not just your IT guys. The same could be said for SAP (Systems Applications and Products in Data Processing). When SAP doesn't work it's not instantly IT's problem, it's everyone's. IT ensures that SAP is running while everyone else in your company is using the program. A great quote from Jeff Hall during this webinar relating to security was, "You can't just say 'we protected A so everything else will be fine." During the Solar Winds attacks, one company wasn't affected by the hack. That company was the Internal Revenue Service because they had some of the most restrictive network egress rules of any organization on the planet. No security system is perfect, so you have to go beyond being FISMA, HITRUST, or PCI compliant.

Conclusion

Security is never going to be perfect. As technology continues to grow and advance, we will need to constantly refine our methods of security and risk assessments. We have to go beyond the basics of protection for our information. If we are not compliant with our security systems, this allows for attacks that can damage your company's reputation and clients' futures. 95% of organizations have the tools they need to be secure, but they are not using them properly, whether they are not setting it up correctly or monitoring it properly. Nowadays, we can no longer say "I'm sure things will be fine" concerning security but rather "Are we prepared for future attacks." By being compliant and focusing on risk assessments, you very well should be.