



## We Must Be Secure .... Right?



So you have taken the steps outlined for you. The firewalls are installed. You have multiple intrusion detection sensors both inside and outside your infrastructure and the virtual private network encrypts and secures your data between all satellite offices. You have taken all the necessary steps your long-term, Fortune 500, consultant partners suggested. You have been assured that your data and that of your customers is now secure. Your newly hired security specialist has taken the position reserved for the programmer that would have shortened the development cycle for your highly touted electronic commerce solution. You need this person now that you have the technology infrastructure in place to secure your environment. The consultants actually said that at least three would be needed as well as a significant increase in your security training budget for existing staff. You have paid their bill and there is an eerie, relative calm that presides over your IT department. The CFO, CEO, and CIO are happy with the investment in light of all the security concerns voiced in today's newspapers, magazines, and television.

But, have you really solved the problem? Is technology unto itself the answer?

The multi-layered approach to defending your environment is right on the money. The vulnerability assessment did find the holes in your infrastructure that now should be plugged. You have employed new anti-virus and content scanning software. The intrusion detection sensors are tuned and configured to pick up the slightest hint of probing, attack or benign packets. You don't mind having this level of logging since more is better than less with respect to security.

A few months have gone by and as far as you know everything is fine. But the IT department is receiving automatic pages every night with ever increasing frequency. They are frustrated with the constant false alarms and false positives that occur. Your new security specialist has vowed to shut off the alarms that are causing the sleepless nights and may have already done so. As far as you know, there have been no malicious penetrations. The excitement created when an actual attack occurs has never materialized. All that money and you haven't been able to enjoy the frantic excitement of turning back an attack. Most of the new staff spend their time watching monitors for security events. Many day-to-day tasks are going slipping behind schedule. Your focus has changed from supporting your internal customers to one of subservience to the seldom yet enormously critical attack upon your infrastructure. Catching the attack creates heroes. You want to be there.

Another month goes by and the IT department has submitted a PO for more storage capacity. When queried, they respond that the multiple new security devices are creating reams of data in the form of logs. When queried further, IT indicates that there is so

much data being generated from the logs that they have neither the time nor the expertise to determine if there are any actual intrusions not being picked up from the sensors. The analysis required to sift through the logs is not part of anyone's skill set. The security that just a few months ago seem impregnable is so complex that your IT staff may be missing intrusions in the incident logs. Meetings are being held in IT to setup off-hour on-call schedules. A request has come through for an on-call bonus structure to be created. A call to your consultants and the advice comes through to now purchase an event correlation engine. The problem is, is that they are very expensive and require training to house your own.

Maybe the advice provided by the consultants wasn't complete. Maybe it wasn't completely focused on you the customer. Most likely, security is only another of their services and not the main focus of their business. Regardless, you have issues that need to be resolved. What is your next step? Can you reverse the spiraling costs that confront you? Why not outsource your electronic security? Can you afford not to?

Physical security is always outsourced in the banking industry. It is the norm in healthcare as well. Almost everywhere you look physical security is outsourced to professionals. Most of the time spent on the job is uneventful but when an issue does arrive, they have the expertise to implement the proven policies, procedures and incidence response to hinder if not completely halt the actual event. Why not do the same with your electronic security? How valuable is your data or that of your customer? What would happen to your company's reputation in the event of an attack?

Security providers have the expertise needed to support and monitor your environment. This is their business. This is what they live for. They provide 24x7x365 monitoring for not only you but other customers. The experience they gain from one customer is automatically applied to the next. The parameters they use and thresholds they set on your devices are based upon standards and experience. The alarms are configured correctly. The level of your security is actually increased. The event correlation engine they use automates the process of log analysis and strips the data of the false positives. The amount of storage required is immediately reduced.

New vulnerabilities, new hacker tools, new security products, new patches, fixes and service releases are the responsibility of your security partner. The costs for these tools are spread across many customers. Training, testing, and running through attack scenarios is their way of life. The monitoring they provide is an umbrella of electronic and intellectual security that proactively protects your mission and business critical environments. The sheer volume of events, data, and alarms produced by the firewalls, intrusion detection sensors and other devices will be reduced by your professional security partner. They will provide the ability to intelligently monitor events and transform them into alerts. Your partner should be able to automatically select and correlate alerts from multiple devices, from multiple logs, that in combination describe a security incident. They must be able to automatically track security incidents early on to limit and prevent damage to your infrastructure and subsequently to your brand name and

customer's data. Security providers must be able to minimize your vulnerabilities and they will. It is what they do.

The position you were going to use to speed the development of your ecommerce solution is now available. The training dollars can now be allocated to the marketing department to get the word out on your new product line. Your day-to-day IT tasks are once again being completed.

Don't overburden your already understaffed IT department. Outsource your security management and monitoring to professionals. Let them protect your revenue-producing IT infrastructure. Let them optimize your existing security technology investments. You wouldn't have a teller transport your money from one bank to another. You wouldn't have a nurse provide security in the emergency room. You wouldn't have your admin guard the building at night. It sounds ridiculous but the analogies are sound. Outsourcing your security to professionals is the best insurance policy you can invest in to protect your company's future.

Jeffrey S. Bardin, CTO  
Treadstone 71  
jbardin@treadstone71.com