

Security Blind Spots

By Augusto Paes de Barros – ISSA member, Brasil (Sao Paolo) chapter

Organizations tend to have systems and devices that seem to be excluded or overlooked from the main security efforts and processes – security blind spots.

My goal is to illuminate some overlooked areas of organizational behavior. I am attempting to inform CISOs and others with security responsibility that there are probably a few dark corners within their organizations, harboring great potential risk exposures. I am not trying to change assessment methodologies; neither am I indicating formal standards to be used. It is more about behavioral change.

You probably can list off the top of your head all your network's perimeter security controls or even those in your Active Directory. However, many organizations have areas that seem to be excluded or overlooked from the main security efforts and processes. I call these *security blind spots*. Main-frame systems and utilities, physical access controls, support tools – these are some areas often forgotten by the Information Security department, incurring unforeseen risk to the organization. In this article I will offer some reasons behind these security blind spots, where they most likely occur, how to find them, and how to avoid new ones.

Why the blind spots?

Several reasons can lead to the overlooking of blind spots, the most common being a misconception of a device or application's potential impact to the information infrastructure. Typically misconceptions are formed through (1) lack of knowledge about the importance of the systems to critical business processes, (2) shared resources, (3) systems maintained out of the formal IT responsibilities, and (4) distorted vulnerability information about specific technologies, devices and applications.

Knowledge about a system's importance

While working on a number business impact analysis projects, I have noticed a widespread tendency: when identifying a critical IT system to a specific process, people tend to forget basic resources, as if they imagine that an incident will not be able to affect them. The most common would be email systems, printers, Internet access and files stored in individual workstations. Additionally, some systems are developed/deployed outside the IT group's control (see Shadow IT below).

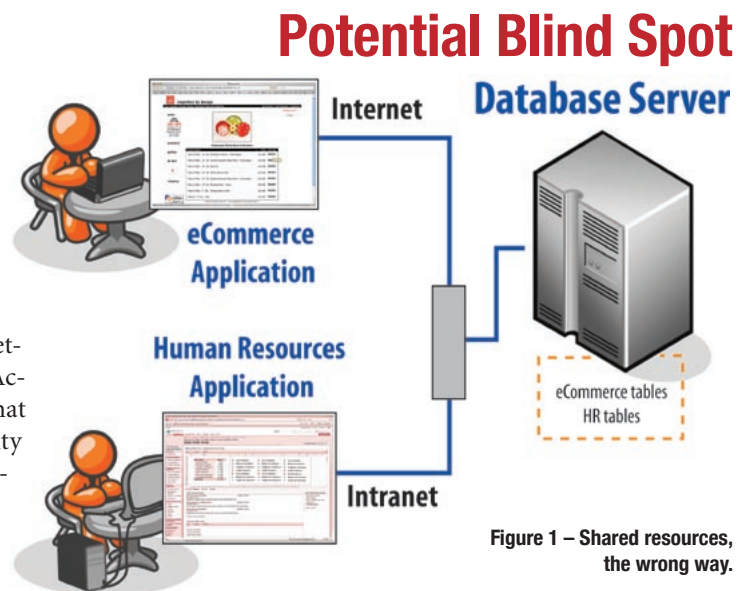


Figure 1 – Shared resources, the wrong way.

Additionally a system's importance to the business process may grow so slowly that nobody notices how critical it is becoming. If the IT group is not aware and the business group does not tell, chances are that those systems will be left out of disaster recovery plans and overlooked by the security infrastructure. An incident, however, will soon illuminate these deficiencies.

Shared resources

Because of the need for optimizing costs and resource utilization, it is very common to install applications on shared servers or databases. However, it is not hard to find two applications with information of different sensitivity levels and different user groups (e.g., Internet users, internal users) utilizing the same server, database or even database instance. See Figure 1. This practice can make vulnerabilities from one application affect the risk level of the others sharing the same resources. I once found an SQL injection vulnerability in a small, internally developed web application designed to sell subsidized movie tickets to the employees of a large company. The application was so trivial that it was seen as merely a “web page,” not an actual application with database access and so on. By exploiting that injection vulnerability I was able to ac-

cess critical databases running on the same server, including one with data about employee 401(k) plans. Shared resources contributed to a case of confidential information exposure.

Resource sharing goes beyond servers and databases, and few IT professionals can see how deeply network resources are shared. It is quite common to find networks designed with only one goal: unlimited connectivity. The compartmentalization of IT environments by different levels of sensitivity, types of users or information is one of the most important steps in architecting a secure corporate network, but it is frequently forgotten during the design of corporate backbones.¹ An increasingly common example would be new VoIP infrastructures being deployed over already established data networks which are managed through different aspects of connectivity. I have heard telecom professionals referring to data network specialists as “data cowboys” because of the different way each group considers things like availability, shared resources and quality of service.

Shadow IT

There is also the problem of IT solutions created outside of the formal IT group – the Shadow IT. Today, almost all business units have people with a good understanding of IT solutions. Those people, however, are not typically cognizant of the management and control processes required to keep IT running, and often think that involving the IT group with their plans will just bring more bureaucracy. They see their technology as something that is not big enough to necessitate IT management or concern, so they build and manage it themselves, using computers under their desks and connecting everything with an Ethernet jack to the corporate network. The most common cases include the following:

- **Financial systems** (and several companies are now feeling the pain from SOX), especially those developed as an Excel spreadsheet and evolving into a shared Access database²
- **Physical access control systems** – who manages the badge reader system? Is there a process to periodically review its database? It is common to find that people from Security (not Information Security) are installing systems to control those devices without working with the IT group.
- **Voice (PBX, IVR, VoIP) and SCADA³ systems.**

In the health industry the diagnostics devices support systems are also a common example.⁴ I have seen a single workstation cause havoc on a hospital network just by answering

There is the problem of IT solutions created outside of the formal IT group – the Shadow IT.

ARP requests destined to diagnostics devices, causing a denial of service condition. The IT managers discovered only at point of failure that those devices were connected to the corporate network, the same used by regular office workstations, raising security issues not only related to the availability of systems but also regarding the protection of patient information privacy.

Vulnerabilities on those systems represent a huge risk to organizations, but are frequently overlooked and left out of the security assessment processes. They are managed by people outside the traditional IT group and are often hidden from the security folks,⁵ especially in companies where the security group is under the CIO. Those systems are usually left out of the regular IT management processes as well – change management, problem management and incident management. The unknown interaction of these systems with the rest of the IT environment can create unforeseen surprises for both sides: side effects ranging from network changes that did not consider them to incidents without clear causation (the device causing the incident not being on the list of the managed systems, hence, being excluded from a root cause analysis).⁶ Considering that one of the best practices is to integrate security into the IT control processes already in place, those systems end up hidden from security too. It is just not possible to control something you do not know about.

The mainframe

Another well known blind spot is the Mainframe, present for decades in the corporate environment. Considered to be a very secure platform, it is usually spared thorough security assessments.⁷ In truth, most of them are left out of the assessments because security professionals today come from the distributed computing world (i.e., PCs, Unix), lacking the necessary skills to perform security assessments on the “big box.” Some applications pass through user profiles reviews, but they are seldom verified in a secure architecture/coding perspective.

The production environment of the mainframe can also be a huge source of security risks, with numerous production or support analysts directly accessing data with support tools.

1 Tom Adams, et. al., “Network Segmentation,” www.techworld.com/whitepapers/index.cfm?whitepaperid=2986.
 2 Luke Chung, “Database Evolution: Microsoft Access within an Organization’s Database Strategy,” www.fmsinc.com/tpapers/genaccess/DBOD.asp.
 3 David Maynor and Robert Graham, “SCADA Security and Terrorism – We are not crying wolf!” *Black Hat Briefings DC 2006*, www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf, 2006.
 4 Ellen Messmer, “When medical-device equipment gets sick,” [Networkworld.com, www.networkworld.com/weblogs/security/005694.html](http://www.networkworld.com/weblogs/security/005694.html), July 2004.

5 Joe Sauver, “SCADA Security,” University of Oregon Computing Center, www.uoregon.edu/~joe/scada/SCADA-security.pdf, July, 2004.
 6 Hank Marquis, “The Rise of Shadow IT,” *CIO Update*, www.cioupdate.com/reports/article.php/11050_3633056, September, 2006.
 7 Dan Kaplan, “Remember the Mainframe,” *SC Magazine*, www.scmagazine.com/Remember-the-mainframe/article/34180/, November, 2006; Timothy P. Morgan, “PowerTech Issues Third Annual State of i5/OS Security Report,” *IT Jungle*, www.itjungle.com/tfh/tfh110606-story03.html, November, 2006; Brian Currah, “MVS: Mainframe Virtual Security,” www.perfassoc.com/jsc/pdf/papers/mvs_security_paper_02.pdf, 2002.

I have seen a simple support situation become a huge data integrity disaster when a support analyst tried to fix a single data record in a VSAM file from a credit card processing application. This simple data “correction” was able to cause integrity problems to the whole database, making it unavailable for hours while the error was being searched and finally fixed. I developed a benchmark with a number of companies to determine how they were dealing with those support needs and was very surprised to discover that nearly all of them were allowing analysts to access production data – directly in some cases – with hardly any control over what they were doing there. Not only can they wreak havoc with mistakes as mentioned above, they are also in a very good position for committing fraud or stealing sensitive information.

The rush to connect these legacy systems to the new world of Internet possibilities and exploring the new SOA concepts⁸ has also left numerous potential breaches exploitable. Programmers with lack of TCP/IP protocols expertise or who do not understand the security challenges of this new world are creating direct channels between CICS transactions and midrange applications, often with little concern for proper authentication, authorization or auditability. By checking audit logs I have found several cases where a “generic” user was utilized by a system accessing the application on the mainframe with no control over the real identity of the source of the TCP connections.⁹ However, the mainframe technicians do not always know that the TCP socket will be available not only to the target application on the other platform but also to all computers on the same network. The open ports on the mainframe pass all the data received directly to the transactions, the layout of the strings being the only “secret” preventing an unauthorized attacker from exploiting them. On the other side, people from the TCP/IP world think that the mainframe is doing something smart to avoid it, as they always hear “the mainframe is very secure.” This is a perfect example of security by obscurity in its worst form. Thousands of connections come and go to and from the mainframe, from FTP to 3270 emulation (very similar to a Telnet connection), almost always without encryption,¹⁰ the data waiting to be captured by anyone with a sniffer that can decode from EBCDIC to ASCII (mainframes use a different convention to represent characters – a simple sniffer can show you the data in an apparently unreadable format, but you just need to decode it to the other format).

8 “SOAs Meet Mainframe Security,” *SD Times*, www.sdtimes.com/article/column-20070515-01.html, May, 2007.

9 To help the reader unfamiliar with mainframe lingo – CICS is middleware that deals with online transactions on mainframes, something like an application server. CICS transactions can be called by users who will provide parameters and receive results after the transaction is executed. Under normal conditions the security system (like RACF or ACF2) will check if the user has the permissions to execute that specific transaction. This is how CICS transactions are made secure. Those transactions are made available to systems running on other platforms through a TCP/IP connection (e.g. CICS Sockets). One of the ways to set this up is to define a generic user on the mainframe that will be used to execute the transactions from this socket.

10 www.greebo.net/2007/12/21/reaching-for-the-high-hanging-fruit/; www.greebo.net/2007/11/18/lets-talk-mainframes-for-a-bit-part-1-background-and-auth.

Solution - avoidance

How can we shed light into those blind spots within our organizations? Blind spots occur mostly because of three things:

- Lack of processes
- Lack of information about business and IT environments
- Lack of organizational or technical knowledge from the security team

Lack of processes

To deal with the lack of processes, it is necessary that the security group be empowered to work with business units and to participate in their decisions in order to fully understand the risks involved. Only by establishing a continuous cooperative relationship between business groups and the security group will it be possible to accurately develop a comprehensive security plan. It is essential that the organization clearly states its policy about information security responsibilities. It is necessary that everybody is aware that *every* IT asset must be known and integrated into the IT management processes of the organization. IT processes, procurement processes and project management methodologies have several decision gates where people need to assess the completeness of tasks and information assessments before proceeding. Security can be quickly integrated in those processes by including checklists and verifications at those decision gates. Change management, IT expenses and project chart approvals are good examples of decision gates that can be used in this manner.

To obtain a better view of the network environments, it is important to verify if the current asset inventory processes and configuration management data bases (CMDB) are being updated and cover all parts of the organization. To be sure that you are aware of everything connected to the network, active scanning and passive network monitoring should be used.

Lack of information

There is also the information about what the business units are doing. Besides empowerment, the security group should routinely participate with the units. The business unit members need to view the security colleague not as someone to ask for an approval *after* everything in a project has been completed but as an active participant. Start asking the units what they are doing, what all those projects are about, which technology they are using, and so on. Do not expect people to remember to invite the security group to their project meetings if the group is not interacting with them on a day-by-day basis. One of my favorite solutions is to have liaisons in the security group responsible for making the connection with each business unit within the organization. Smaller organizations can have just one or two people for all the BUs, depending on the number of projects and initiatives they will usually work on.

Lack of knowledge

Finally, there are those blind spots caused by lack of knowledge about the overall technical architecture being used by the organization. Specialized technical professionals, like firewall and RACF specialists, are very important to the organization; but it is equally important to have someone with an overall view of the integration of all different technologies under a security perspective. This person needs a mix of skills like software development security, network security, access control concepts and, most of all, cannot be afraid of new (or very old) technologies. Be prepared: professionals like that are not common. Also remember that you need security knowledge for all technologies being used by the organization. If you have a mainframe shop, you should have someone on your team with mainframe security skills.

Most blind spots are born from business initiatives. A project is started and finished without involving security (or IT) and something new is brought to the IT environment without the proper assessment of its vulnerabilities and related risks. To ensure that Security is following projects like this, put some experienced generalist professionals on your team as liaisons to the business. They can look at the big picture without the narrow focus of the specialists.

Conclusion

The most important thing to do when trying to fix blind spots is to look for them. You cannot fix what you do not know is broken. Take a look at what the organization is doing and determine if the security aspects have been verified for all those initiatives. If you discover an ongoing business project that you had not heard anything about before, there are probably some overlooked blind spots there. When you listen to specialists talking about “being closer to the business,” this is what they are talking about. Follow business initiatives closely and you will be able to identify the most probable blind spots. By taking this holistic approach you will be able to shed some light on those dark corners and find things that you never thought that could be there – before they ignite and become big problems. It is more about behavior.

About the Author

Augusto Paes de Barros, CISSP, ISSAP, has been working with Information Security since 2000 as a consultant, security manager and CSO. He currently works as Security Consultant for Tempest Security Intelligence and is the committee director of the Brazil-SP ISSA Chapter. Augusto has published articles in several specialized magazines and websites. He may be contacted at augusto@securitybalance.com.

