

The Inside Threat

By Angus MacDonald

What would secret agents do to subvert your network? Hire a bunch of great-looking crypto-security athletes, who would rappel down from a stealth helicopter and make off with a terabyte of your most valuable information on a key-fob storage device?

What would secret agents do to subvert your network? If you believe Hollywood, they would hire a bunch of great-looking crypto-security athletes, who would rappel down from a stealth helicopter and make off with a terabyte of your most valuable information on a key-fob storage device.

The scenario really isn't realistic, but not for the reasons that you think. Hollywood could not make a movie about the subversion of your network because Hollywood needs gun fights and explosions, and simply put, that's not what agencies like the Central Intelligence Agency (CIA) do for a living. More on that later.

Assembling the castle walls

In the last decade, information security (IS) has been targeted at protecting the integrity of data, within your structured data in warehouses and archives, in email repositories, and in the bulk of the unstructured digital documents hidden away from outsiders. Much of the effort has been based on perimeter security – protecting your data from outsiders trying to break into the network. This is an understandable response.

To today's IS executive, perimeter security is a sophisticated notion. In the days of static information in times past, the moat metaphor, hardening the outside of the corporation, was a great approach. But a static boundary is not the reality we work in today. There is no one physical place where people always work. From laptops to home desktops to Internet cafes, many workers are willing to work at a distance from the castle.

The perimeter is porous, in that the mobile corporate workforce, and the partners they collaborate with, have made it difficult to locate the perimeter precisely. When you add consultants, customers and outsourced business providers, the job of the IT department is to enable that work, not shut it down. So the perimeter is now a set of concentric barriers, around the corporation for certain, but also

around departments, workgroups, individuals and, in the extreme, around bits of data.

Consequently, investments have gone into protecting data from malicious outside attack. Driven by regulatory concerns from United States laws such as Sarbanes-Oxley (SOX – protecting confidential

I recommend using a certified system that takes the file system properties, adds metadata, and secures the tags. While you might rely on the document creator to provide the initial tags for a document, an automated system builds a more extensive set of tags that enhances the work of the employee.

financial data) and the Health Insurance Portability and Accountability Act (HIPAA – protecting confidential healthcare information), these investments have so far been successful at managing liability and increasing controls on identity theft, corporate espionage and fraud. However, the question from above remains: How would people go about stealing or polluting your most valuable data?

The enemy inside the gates

If you add sabotage, negligence and human error to the accepted estimates of organizations' monetary loss to fraud, you have numbers that can grab the attention of any boardroom in America. IS execu-

tives need to pay attention to the numbers pertaining to insider activity in the same degree that they examine outsider threats.

Who is this insider? In fact, it is all of us, and any of us. A recent study conducted by the US Secret Service and CERT showed that “insiders” are mostly male; are 17 to 60 years old; half are married; and they represent a variety of racial and ethnic backgrounds¹. Except for the fact that insiders are mostly male, the rest of the parameters point to almost anyone in the workplace.

That’s where the CIA comes in. It is far easier for a secret agent to subvert a willing, or unwitting, corporate insider to do his or her bidding, than it is to covertly intrude, physically or electronically, into a network. In fact, the US intelligence community believes that in the last two decades, more harm has been done to US national security by the likes of insiders like Aldrich Ames and Robert Hanssen, than by any other type of security breach. These long-term insiders sold and gave away a tremendous volume of “secret” material that directly damaged their organizations.

While it’s difficult to place damage to national security on the same page as damage to corporations, there is a price that the private sector pays for insider activity. Personal financial gain and motives are often not the primary motivating factor in insider cases, according to the Secret Service / CERT study. Most of the cases arise when an unhappy employee is seeking revenge, or perceives that he or she has unfairly borne a negative event. And while financial motivation was not the driving force behind the acts, the study goes on to indicate that in more than 80 percent of cases, the victimized organizations did experience financial loss².

Know what you control... Control what you know

So we now know that it’s more than just building a moat – you may be keeping some bad guys in as you keep some of the bad guys out. What do you do about those bad apples, then? In my work with many companies over the past few years, I’ve seen low tech and high tech, I’ve seen policy and process. Short of the low-tech solution of epoxying USB drives closed – and I have seen that – the real answer is a balanced approach.

Identify the relevant data

The data I have been referring to is all of the digital data on your network. It is any data that is created and held in both structured and unstructured forms. Data in traditional database systems makes up much of the structured data. However, research suggests that the great majority of business is conducted with unstructured information. Unstructured data is on documents, reports, spreadsheets, Web pages, images, and audio or video files. Even more unstructured data is in the terabytes of electronic mail and messages that sit on corporate mail servers.

Much work has gone into the protection and security of structured data. However, a motivated insider malcontent could easily export transactional data (thought to be locked down within the database) into a simple spreadsheet or log file. There you have, in essence, unstructured data that is just as valuable and just as damaging as its structured sibling. As you begin to head down this path, consider the ease with which derivative data may be created, and be sure that form of data is included in your plans.

1 http://www.secretservice.gov/ntac_its.shtml

2 http://www.secretservice.gov/ntac_its.shtml

Classify your information

You should start your process by identifying the information that you have in-house. Information represents strategies, transactions, customer relationships, supply-chain activities, market trends, project status, financial performance, and proprietary knowledge, just to name a few key uses. There are any number of security classification systems or protocols, and they can be as simple as a binary “Non-public Information” and “Unclassified,” or highly structured and complex. And there is the classification scheme as defined by the National Institute of Standards and Technology (NIST). It is well documented and clear, and the classification levels are published and well detailed.

Classify your network

Some of you may think I am reverting to the castle-and-moat approach. I’m not – but it’s good to know where the authorized or safe places on the network are, for the previously classified documents. These locations on the networks include the servers, data repositories, storage devices, and in some cases the desktops, laptops and mobile devices where data may reside. This classification is for both “good” places to be, and “bad” places not to be. As such, if there are places within your network that can be identified, you should tag them as places where such levels of classified information should be, and sometimes as places that any information should never be. For instance, you might decide that records should never be saved on a portable “key fob” device (if that’s your policy), and this location should be identified appropriately.

Tag your documents

Once you know the classification scheme of your organization, and you know the authorized and unauthorized locations where documents may flow, you must tag those documents in order to connect your policies. Tagging may be done by hand, where a group of individuals, often within the General Counsel’s office, review and index each document and item of correspondence. This is an expensive, time-consuming, and often error-producing process.

The more accurate and cost-effective method for tagging your documents is at the very time they appear on your network. This can happen at the first “save,” at subsequent modifications and saves, or when the document first arrives as an attachment, and is saved to your files. The document originator is best positioned to determine the scope, place, time and sensitivity of the document he or she is creating. In so doing, that writer is taking only a few additional moments to place tags that can later be reviewed manually or in an automated fashion.

The highest level of tagging is all automated. At the time of document creation, the system (network) itself can tag the document with time, date, device, author name and other indicators – in many file systems this is currently performed for structured and unstructured files. An approach I recommend is using a certified system that takes the file system properties, adds metadata, and secures the tags. While you might rely on the document creator to provide the initial tags for a document, an automated system provides verification of that person’s markers, and builds a more extensive set of tags that enhances the work of the employee.

For instance, an administrator who creates a file of an individual health record may tag the file “Confidential” based on her knowledge of its contents. An automated system can read that initial set of tags, and move the file to “Secret.” This would occur because an

existing security policy indicates that patients with a certain pattern of treatment (shown in the document contents), seen over a certain period of time (from the metadata), and seen at a certain clinic (also the metadata) should be classified Secret. All of this is based on the then-current policies of the healthcare organization. While the creator sets the original tags for a document, the automated system enhances those tags within the system, and without interrupting the workflow of the administrator.

Track data flows and audit

With documents tagged, observe the flows. This observation may be apparent to the system – the system tells the employees that it’s watching, or the system may be invisible. I call this the “Velvet Glove.” It is important in a data policy and tagging system that the system does not force the employees to interrupt their optimized workflow. If the workflow works, it should continue. The best automated systems today can track what happens to data, and where data flows, all in the background. As the system tracks, it learns how the flows are going. And as it learns, it can update the classification scheme and the location parameters that were previously set.

An audit based on a thorough understanding of the patterns of data flow may reveal that some of your earlier assumptions were invalid. For instance, you may have earlier concluded that documents saved while in a local coffee shop are suspect by default. However, this pattern could show that this activity is consistent with lunchtime habits of the design department, where all hands go to lunch and continue to brainstorm on the wireless network in the shop. It is up to you to decide if that activity is legitimate. With the underlying system you’ve put in place, you have data upon which to make a case, or suggest an exception.

Enforce your policies

Once you understand what is happening within your network, you must take action to correct process gaps, procedural irregularities and intentional violations. I have had the pleasure of working inside of and with organizations that have some of the most dedicated and passionate employees and partners in the business. My experience in cases of “irregularity” is that each and every one must be addressed

– both the inadvertent and the criminal. Your policies and all the hard work you did to implement them will be moot if people don’t feel the impact of the program in correcting all types of violations. Simply said, fix the unwitting problems and prosecute the willful violators. That prosecution not only stops the breach, but also sets the tone throughout the organization and beyond. Your definitive action may be a signal to others, and a sign to regulators and criminal prosecutors that your company takes its responsibilities seriously, and therefore doesn’t require “assistance” from judicial or legislative agencies.

Conclusion

In today’s climate of increased regulatory as well as competitive pressures, it’s easy to focus on the threats to the organization from the outside, and ignore other real and expensive threats from the inside. Most books and movies in popular culture show the fight between the good insiders and the evil outsiders. The *Mission: Impossible* movies have glamorized the threat, and consequently we have erected walls and borders in the physical world, beyond the movie screens. In a similar way, we have built moats and castles in the world of Information Security. However, there is another threat, and we must balance our deployments of policy, technology and energy appropriately, between the outside and the inside threat. It starts with the recognition of the problem, and then a few implementation steps in order to keep ahead of the game. You must classify, preferably at the source of creation of the data. You then must audit usage, and finally you must enforce the policy, with an understanding of the patterns of use.

No guns and explosions, but then again, that’s how we will be most successful, and live to watch the stories unfold another day.

About the Author

Angus MacDonald is the CEO of Mathon Systems. He has more than 20 years of business experience in enterprise software and security, in a number of private and public companies, including TIBCO Software. Dr. MacDonald holds a BSc (Hons) and PhD in Electrical Engineering from Edinburgh University, Scotland.