



Raymond Pompon

Senior Security Officer - HCL CapitalStream

About the Author

Mr. Pompon has nearly 20 years of experience in network security. For six years, he was president of Seattle InfraGard, representing the state in a variety of cyber-security events and exercises with the FBI, DHS, and the US Secret Service. He is a lecturer and is also on the board of advisors for both the Information Assurance and Cybersecurity Certificate Program and the Information Systems Security Certificate Program at the University of Washington. Mr. Pompon is a Certified Information Systems Security Professional and a Certified ISMS Lead Auditor.

Information Systems Risk Management – The Challenges

Our business unit just completed a comprehensive risk analysis for our technical infrastructure. At the conclusion, I gave an executive briefing on our findings. As my first slide titled *Top Risks to Our Organization* came up, the most senior executive in the room quipped, “Is this about our competition?” It was a funny moment, but it cut to the heart of what risk analysis is all about: perspective. From my point of view, hackers and cyber-criminals are the biggest threats to our organization. To the people really in charge, it is just one of a dozen worries on their list. It was a good reminder: risk is relative and it must be managed in a manner most appropriate for the organization.

The CapitalStream business unit designs and hosts financial systems for some of the largest banks in the world. This means we not only need to maintain the smooth operations of vital business processes for international banks, but also need to protect millions of dollars of digital assets from cyber-criminals. With that job comes

a responsibility to manage risk to the satisfaction of our customers and external auditors in accordance with the industry best practices.

Risk management, whether it involves technology or investments, is about avoiding unnecessary costs while maximizing profits. Because we provide an affordable alternative for our customers’ IT departments, our team keeps a careful eye on how we spend money. Risk-reducing safeguards are expensive, especially technological safeguards like firewalls and encryption systems. Accordingly, we prioritize our efforts in order to manage the most dangerous risks. This requires a thorough, precise, and realistic risk analysis. However, doing a high-quality risk analysis presented us with many challenges .

First challenge – what should be protected?

Since it is impossible to defend all the assets from all threats at all times, we need a list of the systems and data that need protection. Since every organization has different goals and priorities, this list is unique. As a security consultant working with a large municipality on risk assessment, my client told me they did not care about protecting the secrecy of their data. As counter-intuitive as this seemed, it made

Since it is impossible to defend all the assets from all threats at all times, we need a list of the systems and data that need protection.

"Every bit of data ever produced on any computer is copied somewhere. The digital economy is thus run on a river of copies." Tracking specific pieces of information on a free-flowing river of copies is indeed a grand challenge.

sense. Because they were a government entity, all their documents were subject to public discovery and review. Therefore, the analysis was scoped to examine the integrity and uptime of critical systems.

We already defined the CapitalStream business unit goals quite clearly. Since we host both HCL software as well as other large complex financial applications, such as Misys, it is important that we are worthy of our customer's trust. Our three primary security goals are:

1. The customers alone will decide who can see their data
2. The customers alone will decide who can alter their data
3. Customer data and systems will be available when they need them

We embedded these goals into our training, our documentation, and our operational procedures, which make these goals the perfect foundation for our risk analysis.

Based on our goals, it is obvious that the most critical asset to protect is customer data. The challenge comes from locating that data with certainty. *Wired* magazine founder and visionary Kevin Kelly stated, "Every bit of data ever produced on any computer is copied somewhere. The digital economy is thus run on a river of copies." Tracking specific pieces of information on a free-flowing river of copies is indeed a grand challenge.

The solution we chose was two-fold. First, we created a detailed map of all the systems and data in our organization. Then, we carefully tracked all dataflow and user actions. There are many commercial tools that do this, often part of data leak prevention solutions. Because of our purpose-built hosting infrastructure, we found it necessary to develop our own inventory and data discovery tools. With those tools, we were able to determine the appropriate scope for our risk analysis.

Second challenge – how to model risk?

The recent financial crisis demonstrated the importance of correctly modeling risk. At its heart, a risk model is nothing more than a taxonomy and a method of measurement that provides a picture of the chance and magnitude of potential damaging events. All major compliance requirements like ISO 27000 or GLBA, require a foundational risk analysis based on an industry standard model. Without a model for guidance, a risk analysis can become distorted by individual biases and selective perception. This is especially true regarding cyber-risk, which is complicated and non-intuitive compared to physical risks.

There were many IT risk models available to choose from, including ISO 27005, OCTAVE, and Microsoft's IT Infrastructure Threat Modeling Guide. Since a model needs to reflect reality as much as possible, it was important for us to choose the right model. In our case, no single model accurately captured our two broad

The recent financial crisis demonstrated the importance of correctly modeling risk. At its heart, a risk model is nothing more than a taxonomy and a method of measurement that provides a picture of the chance and magnitude of potential damaging events.

For operational risks, we chose Failure Mode Effects Analysis (FMEA), based on a military operational risk model...

categories of risk:

1. Operational and natural risk: bad things happen
2. Adversarial risk: bad people make bad things happen

The differentiator was modeling a straight probability of dangerous events (like an earthquake or technology failure) versus modeling intelligent adversaries (such as cyber-criminals or malicious insiders) who adapt their strategies. Given this, we chose to use two different risk models. For operational risks, we chose Failure Mode Effects Analysis (FMEA), based on a military operational risk model, currently published as International Standard IEC 60812. The essence of FMEA is to:

1. Break down a complex system into major functional components
2. Map the dependencies, find redundancies, inputs, and outputs
3. Determine the effects of failure of each of the components on the overall system

The value of the FMEA model is that we did not need to enumerate every possible threat. For example, we modeled the effects of a loss of a co-location facility, regardless of reason, with a defined area of impact. This automatically rolled up the threats of fires, cable cuts, lighting strikes, sabotage, and terrorist attacks, into a single risk vector. From there, we looked at the duration of outage – one day, less than a week and longer than a week. Then we repeated this exercise for multiple facilities, computing systems, and dependant services, which quickly gave us an

idea what we could not allow to fail.

For adversarial risk, we chose a game theory threat model with key structural components borrowed from the Microsoft STRIDE threat model and RMI's Factor Analysis of Information Risk (FAIR) model. The goal was to look at how an adversary would attack our systems, keeping in mind their goals, capabilities, and methods. Based on this, we enumerated threat vectors, such as malware injection, physical intrusion, insider misconduct, and social engineering (con games).

Third challenge – using the risk model properly

Now that we had established our models, we needed to populate them with relevant data. The goal of risk analysis is to reduce uncertainty about the future. However, it is worse to be certain about an incorrect future.

To guard against bad assumptions tainting a model, we used a team approach. Various experts from both inside and outside our organization provided direct data or oversight into the risk analysis process. The models we chose automatically articulated all possibilities, thus forcing the team to recheck their assumptions. We also gave our analysis team a set of “worst case” assumptions to feed into the model, which included things like:

- ⦿ What happens when a piece of technology fails
- ⦿ Assume that people will make mistakes
- ⦿ Data may flow to other systems unless explicitly prevented
- ⦿ Things should be considered insecure until proven otherwise

The risk analysis team spent several months on this process, and the final report is nearly 100 pages in length.

Populating the adversarial model was bit a

It is important to examine the trade-offs between a risk and the costs to business. Organizational goals should obviously come first, but some risks leadership may deem acceptable in order to create innovative technology, to expand into new markets, or to provide a richer customer experience.

complex. For data inputs, our team used a variety of data sources regarding attack characteristics including our own experiences in hacker incident response, the recent Verizon Cybertrust breach report, and information from recent network security vulnerability scans. The goal was to use current facts and measurements as much as possible.

For example, looking at the malware threat:

We first examined the contact points where an attacker could inject malware into our network, including: a) Drive-by-downloads (getting infected via a website), b) Inbound Internet connections (a worm infects a server), c) Infected USB sticks, d) E-mail. Each of these contact points has a footprint describing how accessible they are to attackers. For example, the footprint for a drive-by-download included all users who browsed the Internet. We mapped these contact points against the frequency of contact. Following the same example, a recent study by McAfee has shown that approximately 1% of all websites contain malware. Then we measured the

defensive effectiveness for each contact point. For malware delivered by drive-by-downloads, this includes firewalls, intrusion prevention, antivirus software, browser patch frequency, user awareness, and browser configuration. After that, we looked at the impact of a malware infection against our assets and corporate goals, given that we segregate the Hosted environment from where users surf the Internet. We then looked at this for each contact points. The aggregate gave us a measure of how much of a threat malware was to our organization.

We did this type of analysis for each adversarial threat, such as malicious insiders, physical intrusion, or phishing attacks. After comparing all our other risks, we determined where the biggest risks were and where we should first apply additional safeguards.

Final challenge – some risks are worth taking

The work of managing the risks can be commenced once the risk analysis is complete. This involves applying safeguards to reduce risks or altering organizational behavior to avoid risky actions. However, sometimes a risk is "worth it." It is important to examine the trade-offs between a risk and the costs to business. Organizational goals should obviously come first, but some risks leadership may deem acceptable in order to create innovative technology, to expand into new markets, or to provide a richer customer experience. After all, the only way to reduce risk to zero is to close-up shop.

Links

1. Failure Mode Effect Analysis (FMEA) <http://www.fmeainfocentre.com/>
2. Factor Analysis of Information Risk (FAIR) <http://fairwiki.riskmanagementinsight.com/>
3. Microsoft IT Infrastructure Threat Modeling Guide <http://go.microsoft.com/fwlink/?LinkId=154010>
4. Verizon Cybertrust Data Breach Investigations Report <http://www.verizonbusiness.com/worldwide/products/security/risk/databreach/>
5. McAfee report: The Web's Most Dangerous Search Terms http://newsroom.mcafee.com/article_display.cfm?article_id=3526
6. ISO 27000 Information Security Management System (ISMS) standards <http://www.27000.org/>