**Week 3: Monitoring Security Risk**  
Nate Bachmeier  
July 27th, 2014  
CMGT442: Risk Management  
University of Phoenix

# Monitoring Security Risk

It is a widely accepted fact that it is critical to the success of an organization to have security services correctly deployed across their environment. These systems prevent misbehavior either through accidental or malicious intent. After being deployed within an enterprise, security monitoring activities need to be conducted across internal business practices and among external interactions.

# Monitoring Internal Security Risk

For many it is easy to accept that there are thieves that want to steal from their retail outlets or computer hackers trying to break into their network. However it is much harder to think that “good old Joe from accounting” might be plotting to embezzle millions.

## Payroll

The payroll department presents a unique sets of monetary risk to the organization. If an employee is able to leverage an exploit, they directly receive money. The exploitation can occur through technical or process based vulnerabilities.

For instance a technical vulnerability might include a software bug that allows the actor to update a payment or billing amount to themselves or another entity. Common examples include SQL injections and cross site scripting (XSS) attacks (Stallings & Brown, 2008).

To mitigate these risks change management solutions (CMS) need to exist (Marchewka, 2012). For a small organization it can be as simple as an email notification to a leadership team. As the organization becomes larger and more complex so does the CMS. The organization might introduce a multiple authorization policy, such as the manager and skip manager need to approve the pay change (Stallings & Brown, 2008) (Hernandez, 2012). Having an audit trail will be useful when understanding what has happened and how it became approved.

In addition to technical vulnerabilities are process attacks such as collusion and other poor oversight vulnerabilities (Hernandez, 2012). To provide a real world example, a popular bar downtown had designed policy that managers needed a second manager to authorize an expense report. This simple policy kept everyone honest until two of the managers started dating. At that point they began authorized for one each other, eventually collapsing the business.

To mitigate these classes of issues regular auditing both by internal leadership and external consultants needs to exist (Hernandez, 2012). The internal team is there to go over the books and find any obvious signs of accidental or malicious corruption. Later on a given cadence external consultants can validate the internal team is efficient and not corrupt themselves. Another benefit to external consultants is that they are unbiased.

## General Ledger

Similar to payroll, the ledger and accounts payable records also present risk from internal attacks. Dan Ariely discussed such an incident at MCI telecommunication, where an employee in the accounts receivable became overwhelmed by the work. His job was to collect money from overdue accounts. One day he thought, “what if I just set the debt to 0$?” The company would be happy as owed amount has declined, customer is happy, etc. This quickly became a slippery slope and to keep making the new expected quotas had to blank out debt more frequently each quarter (Ariely, 2012).

After discussing his problems with a friend, that friend decided to visit each of the overdue accounts and offer cash settlement offers at pennies on the dollar. Not too unexpected the story ends about 18 months later in court.

Through proper security monitoring this story could have been prevented or at least reduced in damage (Cooper & al., 2005). For instance auditing solutions needed to be in place to detect an unusually high amount of debt being waved. These can be achieved easily by sampling base lines and looking at trend charts, or complexly designed through Machine Learning as a Service (MLaaS) systems (Ng, 2014).

Another issue is that the employee had the ability to clear any debt of any amount. More granular controls needed to exist either in technical road blocks or at least through business policy. For instance having a rule that any settlement over 1000$ requires a supervisor to sign off and log the business justification. In addition to reducing risk per incident, having safeguards as another part of business culture reduces employees “risking it the first time.”

Lastly having dedicated monthly meeting to review the charts could have alerted the stakeholders of the sudden shift in high debt clearance. Other charts such as the volume of approved escalations could have also tipped them off something was wrong.

## Inventory Control

An organization that does not have good security around inventory control will find it difficult to stay profitable or even remain operational. Washington State outlined an inventory management framework as part of the Washington Initiative 502.

According to 502, there are three key phases to where inventory is at risk; production, processing, and retail. At each phase detailed records need to be maintained regarding resources coming in and product going out. If these detailed records are not available, it is easier to misrepresent tax information or have employee’s steal from the organization.

Another mandate of 502 is to use video surveillance of all primary doors. Video feeds need to be watermarked with the date and time, then encrypted to prevent tampering and finally uploaded to a remote location. Having the video in a remote location prevents a robber stealing inventory and the evidence (State of Washington, 2014).

Ideally technology solutions need to be deployed throughout the end to end process. For instance as the product is unloaded into the warehouse it uses RFID chips to record when it enters or exits a room. These signals can then be fed into an Enterprise Resource Planner (ERP) to remove accidental loss. At the cash register a Point of Sale (PoS) system can be leveraged to push updates of which items have been purchased (State of Washington, 2014). Having a continuous electronic monitoring of the ecosystem reduces risk of loss and cost associated with inventory control (Cooper & al., 2005) (Marchewka, 2012).

## Human Resource

The human resource department will have many of the same risks already discussed, and also need to protect against information disclosure issues. To provide an example, the human resource department will have information on employee medical claims or advance notification of potential mergers or other valuable information.

This data needs to be protected through security systems such as encryption, central authentication, and authorized through DRM or related technologies (Stallings & Brown, 2008). Each of these protections will emit audit records that need to be explored and reported on. Anomalies and other unlikely events escalated into alerts for the administration team.

# Monitoring External Security Risk

Risks of an organizations exist within their corporate walls and among their employees, and also with interactions with external users of their services. Many of these users will be honest and legitimate customers, however a handful will be there to vandalize and steal from the company.

## E-Commerce Site

A core area that needs to be monitored are e-commerce sites. If there are vulnerabilities in the service the company could give out bogus refunds, discounted products, or private information such as credit card numbers (Stallings & Brown, 2008).

To ensure the quality of service and the experience of the user, security monitoring needs to be deployed at the networking level of the edge routers (Goleniewski & Jarrett, 2007). Trends need to be evaluated such as high volumes of corrupt or malicious traffic. Denial of service attacks can degrade the service and cause legitimate traffic to use a different provider (Stallings & Brown, 2008).

Another area to monitor is fraudulent activity, such as automated bots in the auctions. It is not fun for people to compete against programs which will cause them to use different providers (Greenstein & Vasarhelyi, 2002). Also having a lot of bots in the e-commerce site is likely to decrease the margins available on the products. For example if a bot detects that a product is mispriced, then it can automatically exploit the incorrect data entry.

# Conclusions

Running a business is a complex task that needs to be accomplished in a hostile environment. Employees will steal and attack the systems the same as external users of the service. It is critical for the success of the organization that security systems be in place to prevent accidental or malicious usage.

While having such systems provides a layer of safety, it is not sufficient and another layer of monitoring needs to be provided. For instance if access was denied to the secure room, notify the security team so they can investigate who was trying to get in. These solutions ensure the business continues running as expected.

# References

Ariely, D. (2012). *Predictably Irrational, Revised and Expanded Edition: The Hidden Forces That Shape Our Decisions.*

Cooper, D., & al., e. (2005). *Project Risk Management Guidelines: Managing Risk in Large Projects and Complex Procurements.* John Wiley & Sons, Ltd.

Goleniewski, L., & Jarrett, K. (2007). *Telecommunications Essentials. The Complete Global Source, Second Edition.* Pearson Education.

Greenstein, M., & Vasarhelyi, M. (2002). *Electronic Commerce: Security, Risk Managemetn and Control.* McGraw-Hill.

Hernandez, S. (2012). *Official Guide to the CISSP CBK, Third Edition.*

Marchewka, J. (2012). *Information Technology Project Management. Providing Measurable Organizational Value, Fourth Edition.* John Wiley & Sons Inc.

Ng, A. (2014). *Machine Learning.* Stanford.

Stallings, W., & Brown, L. (2008). *Computer Security: Principals and Practices.* Pearson Education, Inc.

State of Washington. (2014). *MARIJUANA LICENSES, APPLICATION PROCESS, REQUIREMENTS, AND REPORTING.* Retrieved from https://lcb.app.box.com/adopted-rules