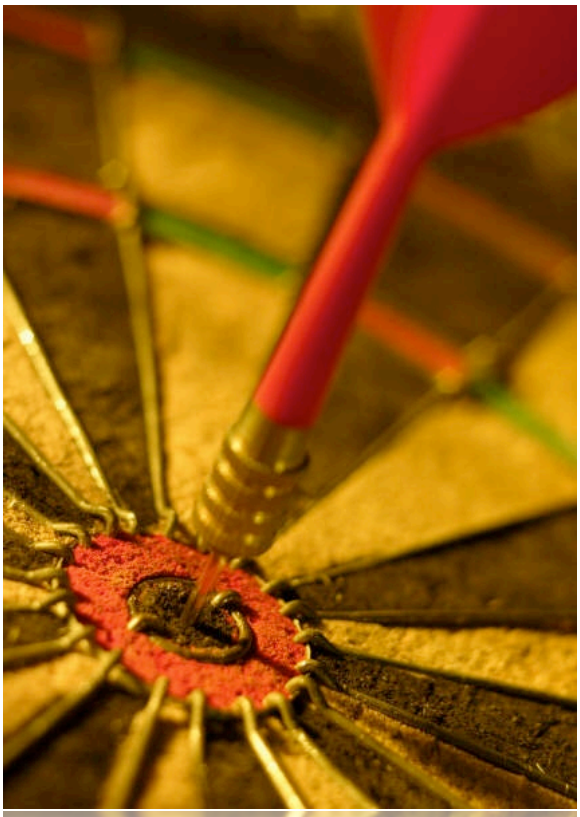
THE 80/20 RULE FOR SECURITY



HOW TO GET MORE SECURITY FOR LESS

By:

Valerie Thomas, Security Analyst, with

Brent Huston, CEO and Security Evangelist

MICROSOLVED INC

MicroSolved's 80/20 Rule for Information Security

These days everyone is expected to do more with less. As a Chief Information Officer (CIO) or IT Manager, you're expected to expand capabilities, embrace new technologies, increase operating efficiency, and keep it all secure. Micro- Solved, Inc. (MSI) has developed the 80/20 Rule of Information Security that proposes the concept that 80% of an organizations' real information security comes from only 20% of the assets and effort put into the program. These 13 security projects will give your organization the most effective information security coverage for the least expenditure of time and resources.

According to the 2009 Data Investigations Breach Report by Verizon 285,000,000 records were compromised in 2008. How did this happen? One of the biggest problems in security today is that organizations don't know enough about what they have. 80% of the compromises detailed in the report resulted from one or a combination of three things; unknown data or location of data, unknown network connections, and unknown access or privileges. In order to de- fend your environment you must know more about it.

Who are we defending against? Over 90% of the compromised records that Verizon details were from organized crime. The true threat does not come from teenage hackers with nothing better to do. It comes from sophisticated organizations that are looking to make a profit. However, it's getting a bit more difficult for them to do so. The value of personal data (social security numbers, etc) is decreasing rapidly because it's easy to obtain. Corporate secrets are the latest moneymaker. Source code, schematics, and blue prints are a few examples of what attackers are attempting to locate and sell to the highest bidder.

The most effective way to secure your environment is to know it. But where do you start? These projects, once completed, should allow CIO's to create an effective, efficient, and standards-based approach to information security.

Project 1: Data Flow and Trust Mapping

It's impossible to protect everything in your environment if you don't know what's there. All system components and their dependencies need to be identified. This isn't a mere inventory listing. Adding the dependencies and trust relationships is where the effort pays off.

This information is useful in many ways:

- If Server A is compromised incident responders can quickly assess what other components may have been affected by reviewing its trust relationships
- Having a clear depiction of component dependencies eases the re-architecture process allowing for faster, more efficient upgrades
- Creating a physical map in accordance with data flow and trust relationships ensures that components are not forgotten
- Categorizing system functions eases the enclaving process

Don't know where to start? It's usually easiest to map one business process at a time. This enables everyone to better understand the current environment and data operations. Once the maps are completed they must be updated periodically to reflect changes in the environment.

Project 2: Risk Assessment and Threat Modeling

Now that we know what systems are present, it's time to take a more in-depth look at them. After completing the data flow and trust maps you now have an understanding of how your systems communicate and support each other. However, there are many factors that are still unknown:

- What vulnerabilities exist on each system?
- Are there security controls that govern system configuration and operation?
- Where does risk exist in the environment?
- How severe is the risk?

Risk assessments are designed to enumerate and prioritize threats and vulnerabilities, examine the effectiveness of the security controls in place, and rate the existing risks in the environment. Completing a risk assessment will answer the listed unknowns. Additionally, it will identify needed policy changes and new policies that need to be created.

The threat modeling process is used to identify and mitigate design security problems that could lead to system compromise. By seeing the system through the eyes of an attacker, organizations can take the appropriate steps to correct any design flaws.

Completing these activities gives an organization a clear understanding of what risks are present and what steps need to be taken to mitigate them. If you've had a risk assessment done in the past go back and review the results. What steps have been taken to mitigate the identified risks? Likely, it will require some updates, though. Risk assessments should be performed periodically and certainly after any significant change to the IT or business environments.

Project 3: Ongoing Assessments of Attack Surfaces

After completing a risk assessment and threat modeling you now have a prioritized list of actions that need to be taken. However, new vulnerability reports are released every day and organizations need to stay abreast of the latest threats to their environment. The easiest way to accomplish this is by performing ongoing vulnerability assessments of external, internal, and web-based applications. Not only does this provide you with a roadmap for mitigation; it also provides metrics that are useful to show progress and return on investment. These assessments are usually performed by a third-party vendor that possesses the proper tools and skill set to effectively evaluate your network. Assessment activities should include vulnerability

assessments, penetration tests, and application assessments. Be certain that the assessment reports contain detailed mitigation strategies. If the vendor is only telling you what the problem is, but not how to fix it, you're not getting a return on your investment.

Project 4: Minimize attack surfaces

After completing a vulnerability assessment you probably have a very large list of mitigations to complete. Want an easy way to reduce the number of vulnerabilities in your environment? By removing non-essential attack surfaces you're reducing the number of attack surfaces (and vulnerabilities) for an attacker to exploit. Some basic steps include:

- Ensure that all exposed forms of remote access are as secure as possible
- Removal of default or test accounts that exist on systems, devices, and applications
- Ensure that administrator accounts don't have the same credentials for multiple systems
- Introduce multi-factor authentication, if appropriate
- Close non-essential ports on Internet-facing and internal systems
- Review and update Access Control Lists (ACLs)
- Remove non-essential software

Some of these activities may introduce new hardware into your environment. Be sure to continue ongoing assessments to identify new vulnerabilities. Use the results of the ongoing assessments to make configuration adjustments as needed.

Project 5: Implement Egress Filtering

So far we've focused on what's coming into your network. However, we haven't discussed what's leaving your network. Are your corporate secrets floating out into Cyberspace because someone is running Peer to Peer (P2P) software in your environment? Outbound, or egress filtering monitors and prevents certain types of network traffic from leaving your internal network.

This solution is very unique to each organization and is based on their business needs. Industry best practices recommend denying all traffic and permitting by exception. This way if non standard software is required, it can be evaluated by the security and IT teams prior to use.

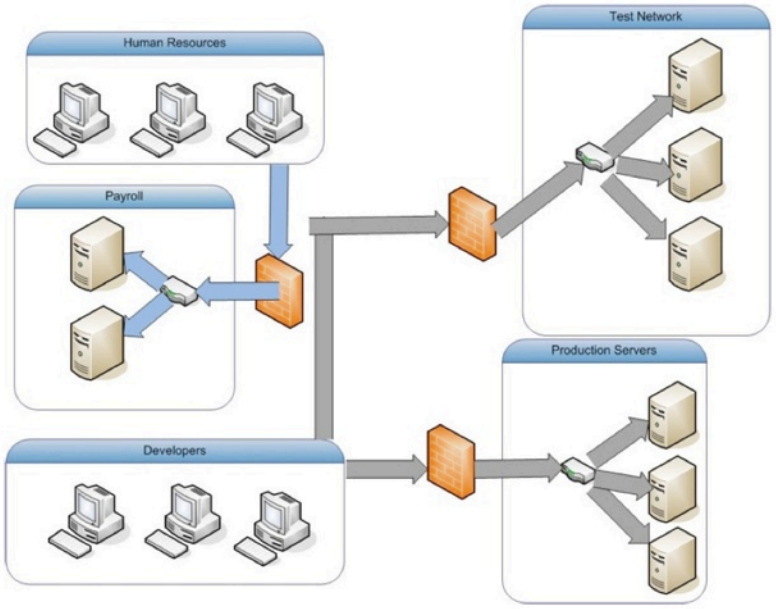
Depending on the priorities of the organization, some may choose to implement web filtering. Web filtering restricts what types of websites users may access, typically through the use of a proxy. If you're not currently restricting web traffic; be prepared for political push back. Users and managers will not be pleased if they can no longer access certain websites, even if they're not job related. Some basics categories to consider blocking are sites known to host or manage malicious software, worms, bots and viruses:

- Gambling
- Pornography
- Social Networking
- Game sites
- Sport games (Fantasy Football)

Implementation of egress filtering is a very involved project that affects everyone in the organization. While it is usually difficult to implement; it's the single most effective control in managing bot-net infections, malware and wide-scale data loss. Not only will you have more control of what leaves your network, but it will also enable your security team to locate malware faster. Most organizations also see a drastic reduction is bandwidth use, which can save thousands of dollars.

Project 6: Network Enclaving

Enclaving, or network segmentation, is the process of making new network segments based on system role, trust relationships, and the types of data processed. These new segments are isolated on the internal network by firewalls and are not accessible from the Internet. We then configure access using deny all, permit by exception. This ensures that only machines with a valid business need can access the segment. The same approach should be taken with the physical location of systems. All employees should not have physical access to the area where these net- work segments reside.



To maximize your return on investment, Role- Based Access Controls (RBAC) should be applied. RBAC is a technical means of control- ling data and resources that users can access based on their position in the organization. The diagram depicts a simple example of RBAC.

The blue arrows depict the components that users with a human resources role can access. Notice that they only have access to segments that are relevant to their job function. They don't need access to the test network or production servers so they are denied at the firewall of those segments. The same goes for those in the developer role. The gray arrows show that this role can access the production servers and test networks, but not the payroll servers.

Enclaving is a very large project and takes considerable time and money. So why do it? Having a segmented network with properly applied controls will drastically reduce the amount of damage caused by an initial-stage compromise. It also drastically reduces the risk of insider threat by limiting the amount of data that an insider with malicious intent could obtain. Combined, both of these factors go a long way to creating a more easily managed and effective information security program.

Project 7: Create Anomaly Detection Capabilities

Signature based technologies alone do not provide the amount of detection that organizations require. When a signature is released for a particular malware program it's similar to releasing a description of a criminal suspect. All of the signature based technologies (Antivirus, etc) are looking for a male with brown hair and brown eyes who is wearing a blue shirt. However, if a slightly different version of that malware program is introduced into the environment that doesn't exactly match the description it will not be quarantined or reported. In this case, the suspect could be a male with brown hair and brown eyes who is wearing a red shirt. The malware still has the same function; it's just slightly altered its appearance.

This is where anomaly detection comes in to play. By looking for abnormal patterns in system, application, and net- work activity it can detect malicious activity and do so with a largely reduced set of data. It will catch new malware (the man in the red shirt) due to a large number of machines attempting to send large amounts of data to a "www.yourhaxored.com". Some examples of anomaly detection systems are:

- Honeypots
- Security Event Information Management (SEIM) Solutions
- Threat management systems based upon anomaly analysis and behavioral testing

Using anomaly based technologies is one of the most effective ways to monitor your environment. These solutions can vary drastically in price and should be evaluated before purchase. Don't forget to include funding for the security team to get training on installation, administration, and backups of the solution.

Project 8: Define Policies and Procedures

Policies are the cornerstone of a successful security program. These policies represent:

- The organization's standpoint on acceptable use of information and equipment
- Responsibilities of management, system administrators, security personnel, and users

Clearly defining roles and responsibilities are essential for success. Not only does this show everyone where they fit in the big picture; it gets them involved in protecting the organization. Not sure if you have the appropriate policies? Here is a quick list that gives you an idea of policies that should exist in your

organization. These policies include:

- Policies, standards, guidelines and procedures
- Risk assessment and treatment
- Threat monitoring
- Security roles and responsibilities
- System logging, monitoring, updating and patching
- System configuration control, change control and life cycle management
- Asset management and protection
- Vendor management
- Personnel/human resources security
- Security training, awareness and education
- Physical and environmental security
- Access control
- Identification/Authentication, authorization
- Privilege control
- Remote access, wireless access, etc.
- Physical access
- Teleworking
- Encryption and key management
- Segregation of duties/dual controls
- Workstation/portable device security
- Acceptable use policies
- Electronic commerce/web site security
- Security incident response and management
- Business continuity/disaster recovery
- System and program testing
- Compliance

Well defined policies and procedures aren't just nice things to have. They are essential to ensure consistency and quality of operations throughout the organization. Already have policies? Re-evaluate them to ensure they are up to date with business needs and current technologies.

Project 9: Undertake Awareness Programs

Traditional security awareness programs can be effective, but if you want to thoroughly educate your employees you need to involve them. Instead of telling them what not to do, teach them to be "net cops." According to recent data that profiled data compromises, your team members (as in humans) are twice as likely to notice strange attacker behaviors, security issues, and other anomalies versus automated systems like intrusion detection systems (IDS) and log monitoring. Teach them what suspicious activity looks like and reward them for reporting it. Some examples of anomalous behavior include:

- Pop-up ads that from sites that have not used them in the past
- The Internet browsers' home page changed without user input
- Web sites that appear to be legitimate but have spelling errors or incorrect logos
- Login pages that have "page not found" errors or just refresh when credentials are entered

Set up incentives for maximum participation. If an employee reports something that appears to be suspicious, place their name in a monthly drawing for a prize. Give away something different each month. The prize could be movie tickets, gift cards, or a special parking spot. An anonymous submission method should also be considered.

The only preventative topic that should be covered continuously is laptop theft. Educate employees on the business impact and costs associated with lost or stolen equipment. The majority of them will be surprised to know that the organization not only has to replace the hardware, but also may have to pay regulatory fines and file recovery charges. Increase awareness by producing short, humorous videos that feature an employee getting a laptop stolen. Include a serious message about how quickly laptops can be stolen and how they should never be unattended.

Project 10: Harden Assets and New Systems

By hardening configurations of network components, systems, applications, and user accounts organizations can dramatically reduce their risk. This also ensures consistency in deployment and maintenance by providing system administrators with a road map that can be applied to each new and existing device. Most importantly, this prevents new vulnerabilities are not introduced into the environment.

Configuration guidelines should be developed in accordance with industry best practices while accounting for specific environmental needs. When completed these configuration guidelines should become the baseline for all new equipment and the goal for all hardening efforts of currently deployed technology.

Configuration guidelines should include:

- Removal of default accounts and unneeded services/software
- Password standards
- Patch management
- Version control
- Account creation and removal
- Testing and approval for new software or hardware

Determining what is appropriate for your operating environment takes time, coordination, and diligence. Most people are resistant to change so expect to get some push-back from just about everyone. Initially users won't

like creating strong passwords and system administrators won't be happy about version control, but with time they will learn to adapt and understand how these guidelines will create a more secure environment.

Project 11: Create and Train an Incident Response Team

Not all incidents can be prevented. In the event that your organization has a security incident you'll need to detect what occurred, minimize the loss, mitigate the vulnerability that was exploited, and restore operations. These actions require a specially trained Computer Incident Response Team (CIRT). For your CIRT to be effective they'll need to possess Incident Response Policies and Procedures. A typical Policy includes:

- The organization's definition of an incident
- When the policy is to be used
- Roles and responsibilities of all parties involved
- Levels of authority
- A severity rating system for incidents
- Types of data that need to be collected
- Reporting chain of command

The CIRT also needs to consist of the appropriate personnel. In addition to a Director and Deputy Director the team should also consist of multiple technical personnel. All lines of business also need to be included:

- Management
- Telecommunications
- IT Support
- Legal Department
- Physical Security
- Human Resources
- Public Affairs

Every line of business will not be used for every incident. However, a representative from each line of business needs to be a trained member of the CIRT. Once your team is established and trained, hold mock exercises to ensure that the appropriate procedures are being followed. These mock exercises can consist of tabletop simulations, role-playing scenarios, and unannounced penetration tests (red teaming).

Project 12: Identify Security Skill Gaps

Throughout this process your security team has likely gained a multitude of additional security knowledge. However, some knowledge gaps may exist. Team members should use previous experiences to identify skill gaps. These skill gaps should be cataloged and matched with courses or reading material. Ongoing education

of the security team is required to remain vigilant against emerging threats, knowledgeable of changing guidance, and aware of new techniques in information security.

New threats are identified daily and updates to compliance requirements, and other baselines are frequent. This is a critical element to maintaining security skills and adequate security postures over the long term.

Project 13: Deploy Rational Cryptography

Deploying cryptography is a must. All sensitive data should be encrypted while at rest and in transit. Particular attention should be paid to laptops and mobile devices. Data is often compromised when these devices are lost or stolen. With laptop theft on the rise, encrypting their hard disks is the best way to prevent data compromise.

Laptops aren't the only devices that need proper encryption. All workstations and servers should have appropriate encryption and key management. Sensitive data should be encrypted in transit by utilizing Secure Socket Lay (SSL) for web applications both externally and internally. A variety of acceptable options exist for secure email transmission. Utilizing Pretty Good Privacy (PGP) keys or x509 certificates are an effective solution for secure email.

This project is saved for last due to the amount of complexity required to implement and maintain. Organizations should select common, well-known key management software that is appropriate for their environment. Most organizations deploy a solution, but fail to properly maintain the keys. Ensure adequate training is provided to your IT staff on key maintenance and reinforce their training with appropriately documented procedures.

Putting It All Together

Chances are some of those projects are already in place in your organization. Perhaps some of them are fully implemented while others are only partially complete. Now that you have a starting point, feel free to use this as a guide to review your current initiatives and their progress. You will find some of these you can do with your current team and others you may want to engage MSI as your security partner. We can work with you and your team to review your current security posture and provide you with a roadmap custom to your organization. From this road map you will end up with a set of projects and the next steps to building a strong information security plan for the future.