Executive Summary

For years, security concerns have been a major driver of IT spending. Every new threat or perceived risk to network infrastructures encourages new vendors and new technologies, each offering another layer of security to respond to a particular threat. Collectively, organizations spend an enormous amount of time and resources deploying and managing security solutions to block malware, protect data, and keep critical business services operating. Yet most organizations remain inadequately protected against evolving and dangerous cyber threats.

One fundamental reason for this disconnect is the sheer complexity of the security management challenge. Each new layer of network devices and security tools adds more information to review and additional management tasks. Network operations and security teams are overwhelmed trying to determine whether existing countermeasures are properly configured to protect. Time is critical as well. Even ‘real time’ detection is not fast enough to avoid a data breach or unauthorized access to sensitive corporate data. As the costs of stolen data and damaged reputations soar, information executives must take steps to augment security response plans with proactive risk prevention.

Fortunately, risk-based security management solutions exist today to make sense of the volumes of data about networks and risks. Incorporating data collection, network mapping, risk modeling and analysis — automated risk-based solutions help bond together the protection technologies already in place, reducing security management costs and increasing the ability to identify and eliminate risks before they can be exploited.

The secret sauce behind the automation of security risk management lies in modeling and simulation technologies. These technologies create a model of complex network architectures using data from every network device. The model can be evaluated thoroughly for security gaps that are created by the intersection of network topology, security controls, and infrastructure vulnerabilities. Attack simulation then runs exhaustive scenarios, checking every possible route and type of attack vector to see where the organization is at risk.

In this whitepaper, we will examine how IT organizations can benefit from the use of risk modeling and simulation technologies to gain a complete understanding of network security risks and solve critical exposures. Risk modeling and simulation can be incorporated into day-to-day IT operations — validating planned network changes, confirming that security controls are working, or performing a full compliance audit without affecting the live network.

Using patented modeling and simulation technologies, Skybox Security provides a complete portfolio of automated security risk management solutions. With Skybox, organizations can automatically examine complex firewalls to find and fix security gaps, troubleshoot complex network availability and security issues, or prioritize vulnerabilities to address before they can be exploited by an attacker.
Introduction

Despite the enormous investment of time and resources in protecting computer networks, organizations remain inadequately protected against ever more dangerous cyber threats.

Since the 1990’s, the traditional security approach has been to build layers of security countermeasures at the network level and at the end points. Popular security controls such as firewalls, antimalware, intrusion prevention systems, data leakage prevention, and others were combined together to offer a ‘defense in depth’ strategy.

Each of these security solutions carries some amount of management overhead — rules to manage, settings to configure, policies to set, and alerts to review. Coupled with emerging threats and the expanding size and scope of most network environments — the IT staff faces a tough challenge to keep networks secure.

As IT teams struggled to deal with the overwhelming amount of management data the security controls generated, organizations started to deploy security monitoring solutions (aka Security Information and Event management — SIEM). These tools aggregate and correlate information from all a variety of security controls, to present the information in one place.

However, since these monitoring solutions collect event-based information, such as security alerts and policy violations that have occurred — they can provide only a reactive, rearview picture of what has happened in the network.

Organizations continue to face high risk exposure to their critical assets and services because:

1. Technical controls are only as good as they are configured. Misconfigurations are common, due to lack of contextual knowledge, frequent changes that impact other security controls, and unavoidable human errors
2. Some technical controls may be missing completely due to lack of understanding of the threat environment, risk level, or lack of budgets to procure or to operate an additional control
3. Patching all vulnerabilities is not feasible in an enterprise environment. Updates may disrupt business operations, and many systems cannot be patched at will
4. Monitoring solutions are only helpful after the attack, and will cover typically pre-defined patterns. If the intruder breaches defenses successfully, the damage can be realized quickly, with little time to contain an attack or limit the damage — even if such attack is detected

What many organizations lack is a proactive security risk management solution, a cost-effective way to improve the security posture before damage has been done. By providing a means to anticipate and analyze security risks — organizations can configure security controls properly, test planned changes for possible security impact, and take action to prevent known vulnerabilities from being exploited.
Consumer Confidence in Credit Card Attack — Life-Like Example

Throughout this white paper we will follow a fictitious story about an organized crime attack by the Red Hack group (or simply, the Reds) that is targeting Acme Power, a large power company that serves millions of households.

Acme Power has built their reputation on customer service initiatives, creating many electronic services for their customers, such as paperless billing, credit card payments, and online account access. Over time, the company has amassed vast amount of consumer information including personal financial information, e-mail addresses, user names and passwords, service history, and more.

Due to concerns around PCI DSS compliance, Acme decided to outsource all credit cards processing to a highly secured 3rd-party credit card processor. Acme keeps the last 3 digits of the credit card number (in the form Xxxxxxxx-xxxx-x380) in their own database solely for reference purposes in communications to consumers.

The Red Hack group is planning an attack that will allow them to steal bank account and credit card information from Acme’s customers, as well as reap a profit by damaging the reputation of Acme Power.

The planned attack has the following phases:

- **Phase 1:** A few weeks before the attack, the Reds short-sell large amounts of shares of Acme Power. In order to avoid detection, the Reds use many traders and numerous shell companies.

- **Phase 2:** The Reds conduct a stealth cyber penetration to the Acme datacenter (details will be provided later), and transmit out a copy of all consumer records, including name, e-mail, user/password, and the last 3 digits of the credit card number.

- **Phase 3:** The Reds divert all the traffic from the real customer support site to a dummy one (by performing “DNS zone transfer attack”), which is prepared in advance.

- **Phase 4:** (performed immediately after Phase 3) The Reds send phishing e-mails to all Acme customers with the following text:

  Dear Mrs. Smith,

  We are sorry to inform you of a security breach involving Acme Power consumer records. It is likely that your credit card account number XXXX-XXXX-XXXX-X380 has been compromised. We are still investigating this breach and strongly recommend that you review the complete information about this issue at our customer support website: www.acmepower.com. Again, we sincerely apologize for the inconvenience, and we can assure you that we are making best efforts to remedy the current situation.

  Customer Services,

  Acme Power

- **Phase 5:** Many consumers log-in to the dummy web site, which provides a believable full customer record using the stolen customer information. Credit card numbers are captured by asking customers to update their billing information to replace their compromised credit card information.

- **Phase 6:** Due to news reports and confusion regarding the security breach, Acme Power experiences a substantial drop in their stock price within days of the attack. The Reds make millions of dollars in profit from their shortselling activity.

How will Acme Power ensure that its network infrastructure cannot be exploited in attacks like the one the Reds plan?
Security Risk Management Overview

Definition of Cyber Risk

Before we describe the security risk management process, let’s establish the definition of “cyber risk”. In risk management methodologies – risk is defined by the impact of a risk event times the probability that the event occurs. In cyber terms, we can refine this definition as follows - cyber risk equals the potential damage to the cyber assets and infrastructure multiplied by the likelihood of a successful attack:

Cyber Risk=Potential Damage x Attack Likelihood.

It can be a very complex exercise for an IT team to try to assess cyber risk manually. To quantify potential damage, organizations can follow various guidelines such as NIST or FIPS to classify assets and evaluate the potential damage if the assets are destroyed or compromised in any way. A comprehensive, current view of the network topology is required, so that the existence and location of all assets is readily available.

A measurement of attack likelihood must take into account three main factors: potential threats, security controls, and vulnerabilities of all systems in the network.

<table>
<thead>
<tr>
<th>Attack likelihood factor</th>
<th>Source of information</th>
<th>Factor controlled by the organization?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threats characteristics</td>
<td>Threat intelligence services; security monitoring solutions</td>
<td>Typically not</td>
</tr>
<tr>
<td>Security controls</td>
<td>Security configuration management systems (typically provided by the security control vendor)</td>
<td>Yes — by ensuring proper configuration</td>
</tr>
<tr>
<td>configuration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vulnerabilities</td>
<td>Vulnerability scanners; patch management systems</td>
<td>Yes — by patching exploitable vulnerabilities</td>
</tr>
</tbody>
</table>

Rating the likelihood of attack requires consideration of all the mathematical combinations of these factors correlated against the current network topology. Clearly, assigning a realistic value of the likelihood of attack requires a sophisticated analysis. Modeling & simulation technologies are key to effectively assess complex attack scenarios. Later sections will explain the use of modeling and simulation in more detail.

The Security Risk Management Process

Security risk management is a process that predicts the risk exposures to cyber threats and enables efficient mitigation of critical attack scenarios before harm has been done. This process enables an ongoing preparedness of the organization to reduce the chance of cyber attacks.
The following diagram illustrates a typical risk management process:

<table>
<thead>
<tr>
<th>Risk Management Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1. Assets and networks mapping | - Identify all systems and networks  
- Discover all vulnerabilities  
- Collect configurations of all security and network controls  
- Classify and evaluate all assets (based on their value to the organization, regulatory requirements, etc.) |
| 2. Risk assessment | - Find all relevant threats, typically from a threat intelligence feed  
- Find all attack scenarios that can be conducted by all relevant threats (internal or external to the organization). Taking into considerations the threat characteristics, security controls  
- Quantify risk for every attack scenario (potential damage X likelihood of successful attack) |
| 3. Prioritization | - For every risky attack scenario, decide on risk treatment: avoidance, acceptance, transfer, remediation  
- For risks that require remediation, plan effective mitigation given alternative solutions, costs, time for remediation and other considerations  
- Verify that planned remediation would actually mitigate the risk down to acceptable level |
| 4. Remediation | - Perform the remediation plan. Typically a combination of patching, removal of services, security or network control re-configuration, and installation of new controls |
| 5. Progress tracking | - Verify that the remediation work was performed as planned  
- Report on progress and trends |
With daily network changes, and new threats and vulnerabilities, an organization’s risk profile is constantly changing. The security risk management process identifies risk exposures at a particular point in time. The time between assessments is critical to overall risk level. Put simply – the longer the time period between risk assessments, the higher the risk level. Diagram 1 illustrates the link between risk level and assessment frequency.

What is the recommended frequency for the risk management process? It depends on your tolerance for risk. A quarterly risk management program could leave the organization exposed to critical risks for 89 out of every 90 days. Many high-performing organizations perform a full cycle at least once a week, if not daily. Clearly, automated analytical tools are required in order to examine an entire network environment at the frequency needed to minimize risks.

![Diagram 1](image)

Acme Power has more than 10,000 employees in dozens of locations throughout the country. The Acme network infrastructure is very complex. It has thousands of servers, over 20,000 end-points (out of which 5,000 are IP-based controllers in their SCADA network), and about 800 network devices (routers, firewalls, load balancers, proxies — from a variety of vendors).

After completing a broad vulnerability assessment project, the Blues realized they have more than 250,000 vulnerabilities throughout the infrastructure. Acme came quickly to the conclusion that patching all those vulnerabilities is neither recommended nor feasible due to the potential disruption of critical services, cost measured in many millions, and the simple fact that the many of SCADA controllers are old and are unpatchable as no reliable patch is even available.

Acme realized that the only way to implement a cost-effective security risk management program would be to utilize an automated solution that can deal with massive amount of information fast, accurately, and routinely — a Security Risk Management (SRM) solution.
Cyber Modeling & Simulation

Modeling and simulation technologies are the ‘secret ingredient’ behind effective security risk management. Modeling and simulation tools are used daily for applications as varied as weather forecasting, power generation simulation, automobile design, civil engineering, forensics analysis, pilot training, and surgical procedures. Modeling and simulation applications allow:

- Prediction of the effects of future situations – Hurricane simulation allows government and citizens to prepare for possible scenarios
- Pre-production testing or assessment – Automobile crash testing helps detect dangerous flaws before production begins
- Process optimization – Modeling power demand helps power generation companies optimize production and distribution to meet demand
- Historical analysis – Forensics investigations may use simulation to reconstruct past events
- Training – Simulated environments offer pilots, doctors, and others a safe and cost/effective means to hone their skills

In the case of cyber security, modeling and simulation technologies offer tremendous benefits along these same lines, such as:

- Prediction of risk exposure before exploitation
- Verification that a planned network change, before the change is made to the production environment
- Optimization of security controls and resources
- Analysis and comparison of complex networks
- Cost-effective training of cyber security personnel

Building a Model

Modeling is the process of replicating or creating a representation of a realistic environment or situation.

In the case of cyber security, modeling is the process of creating a normalized view of the cyber security situation. The model will typically contain information about the network infrastructure, security controls, vulnerabilities, business services, and threats. By normalizing all data into a common format, disparate pieces of information about the environment can be correlated and compared quickly, and updated as needed. The model is an effective way to represent the current state of a network, or to show a past or future state. For example, an organization may wish to model its own network to test defensive capabilities, model an adversary’s network for offensive purposes, or compare models to consider changes and cause-and-effect relationships.
From these data elements, a graphical representation of the network can be built to make it easy to visualize the relationship between network topology, access policies, countermeasures, and so forth. In the case of an enterprise network, the model may need to include hundreds of thousands of nodes, and possibly millions of vulnerabilities. The following diagram illustrates a typical cyber model:
Utilizing an SRM solution, Acme Power created an automatically updated cyber model from a variety of data sources:

- Network vulnerability scanner that provided long list of vulnerabilities for all the hosts in the network
- Patch management system that provided information about all desktops and servers, including installed patches and missing patches
- Asset management that provided asset grouping and classification information, including importance ranking for all the key servers in the datacenters
- Network device repository that provided the configurations of all routers, switches, load balancers, etc.
- Firewall management that provided configurations of all firewalls

The SRM solution was set to collect information from the above sources automatically on a frequent basis, and normalized the data such that every host or device in the network would have an integrated, normalized representation — independent of the source and the vendor.

For the sake of our story, we would continue the example on a sub-section of the network model that included:

1. A DMZ network with one DNS server, and three web servers
2. A Server Farm network that included also a database server for consumers billing
3. A firewall that connected the Internet, the DMZ, and the Server Farm networks

Out of a long list of vulnerabilities discovered in the entire network (over 250,000 instances), one was found on one of the web servers, which is not in use, and had a “Buffer Overflow” vulnerability. This vulnerability allows remote code execution using popular “Root Kits”.

As this specific vulnerability type was found in many areas of the large network, no special attention would be given to this instance, unless the organization had additional knowledge.
Simulation
Simulation is an imitation of a behavior or a process in an analogous way to reality.

In the case of cyber security, simulation allows the imitation of attacker activities, using known vulnerabilities, and information about the infrastructure and security controls in place. The result of this automated process is a set of possible attack scenarios, each a specific set of steps that attackers (humans and/or machines) can take in order to infiltrate the organization’s infrastructure.

By simulating potential attack scenarios against the network model, it is possible to gain a realistic assessment of risk exposure. The combination of modeling and simulation allows complex interactions to be combined outside of the live network environment – so the actual infrastructure is not affected. As there are potentially an enormous number of attack scenarios for a complex network – the attack simulation technology must be very fast and scalable to be effective in real-world environments.

The attack scenario on the left is a typical result of an automated attack simulation. The attack scenario demonstrates how a successful penetration from the Internet to the network can take place:

1. Hacker gains root control of an FTP server (located in the DMZ), leveraging an existing vulnerability that couldn’t be patched due to software dependencies
2. Next, the intrusion disrupts at least one of two application servers that are located in an internal server farms network. Firewalls in between the two networks were not configured to block the access from the FTP server
3. The Consumer Billing service depends on the availability of the application servers, and therefore is affected by the attack

Attack simulation technology is akin to online route planning used by sites such as Google Maps.

Imagine law enforcement personnel using route simulation to predict the possible paths for a criminal who is trying to evade capture. The possible paths would take into account street information, configuration of traffic lights, road signs, street cameras, temporary obstacles, accidents, current location of highway patrol and police cars, and more.

Simulation can find all of the criminal’s likely routes from Point A to Point B given a good model of the environment and assumptions of likely behavior.
Acme Power ran the attack simulation engine of their SRM solution and looked for attack scenarios from the Internet, partner networks, and from internal networks.

The attack simulation came back with tens of attack scenarios from various origins, including the following two attacks:

**Attack Scenario 1**

1. The attacker installs a root kit on the web server, leveraging “buffer overflow” vulnerability. The root kit allows the attacker to execute any code on the web server, and send the results back using the HTTP protocol.
2. The firewall is misconfigured and allows communication from any web server in the DMZ (including ones which are no longer in use), to any of the databases in the Server Farm.
3. The attacker runs a remote query and obtain all customer records including name, user/password, e-mail, credit card account last three digits, last billing info, and more.

**Attack Scenario 2**

1. Attacker uses zone transfer protocol from the DNS server to his own DNS server, which will be used later on to fake consumer web site
2. The firewall doesn’t block TCP communication to the DNS port (53) and therefore step 1 is possible

The security analysts at Acme Power realized that those two attack scenarios combined can lead to catastrophic damage to the Acme business, its consumers, and credit card processors partners.

Once the attack scenarios were provided by the SRM solution, the security analysts could come with a quick and easy remediation plan:

- **Attack Scenario 1** – three alternatives:
  - Remove the unnecessary web server
  - Patch the web server to eliminate the vulnerability
  - Change the firewall configuration to limit traffic only from the required web servers in the DMZ to the specific database server in the Server Farm
- **Attack Scenario 2** – Change the firewall configuration to block TCP communication to the DNS port (53) from the Internet zone

*The Reds attack has been prevented!*
Using Modeling & Simulation for Risk Management

The following table provides a quick summary for how modeling and simulation technologies are used to automate the security risk management process.

<table>
<thead>
<tr>
<th>Risk Management Step</th>
<th>Role of modeling and simulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Risk assessment</td>
<td>Attack scenarios represent all of the possible consequences of threats, vulnerabilities, and the available countermeasures. Each scenario has a likelihood of materializing and potential damage (consequence). Risk = likelihood of scenario x potential damage.</td>
</tr>
<tr>
<td>3. Prioritization</td>
<td>Once the risk to each attack scenario has been calculated, prioritization is made straightforward. Based on resources and time available, the organization will focus on mitigating vulnerabilities and/or configuring countermeasures that are exploitable in the most risky attack scenarios.</td>
</tr>
<tr>
<td>4. Remediation</td>
<td>Using modeling in a “what-if” mode, can allow the organization to check the effectiveness of potential changes based on simulating attacks on a futuristic model — enabling optimization of the proposed changes and verification that the changes achieve their security purpose without unnecessary business disruption.</td>
</tr>
<tr>
<td>5. Progress tracking</td>
<td>Continuous updates to the model allow the organization to automatically identify changes to assets and networks, and to measure the effectiveness of the changes performed, by comparing the attack simulation of the current state to the previous state of the model.</td>
</tr>
</tbody>
</table>

Skybox’s Unique Approach

Skybox Security provides proven security risk management solutions that use network modeling and attack simulation technology to quantify risks and identify proactive steps to improve cyber security.

Technical benefits:
• Automate risk assessments. IT security teams can analyze a complete network automatically and assess overall risk exposure in minutes or hours instead of days or weeks.
• Uncover potential attack paths. Assess vulnerabilities and access routes to find and prevent attack vectors.
• Reduce patching requirements. Focus resources on the most critical, exposed vulnerabilities.

Business benefits:
• Maintain desired risk level. Switch from infrequent or irregular assessments to automatic daily/weekly assessments for continuous risk management.
• Quantify risks. Generates objective risk-based information to support decisions on IT security investments and resource allocation.
• Track operational improvements. Track risk assessments over time to measure effectiveness of security programs.

For more information, see http://www.skyboxsecurity.com/securityrisk
Summary
Organizations looking for ways to stay ahead of cyber security threats are finding it possible to reduce the risk of cyber attacks, even in the most demanding real-world environments. The key is to enhance proactive security capabilities to plan for and take steps to prevent attacks before they happen. Risk modeling and attack simulation technologies allow IT professionals to visualize and simulate the interaction of a complex set of factors — such as network topology, device settings, potential threats, access policies, attacker techniques, known vulnerabilities, and more.

Integrating automated risk-based analysis into daily security and operations procedures is critical. Automation allows for effective analysis of and response to potential attacks against complex network infrastructures. By repeating the analysis as often as necessary, organizations can minimize overall risk exposure and better protect their core business services and valuable information.