RSA

The Security Division of EMC

RSA Solution Brief

Securing Critical Infrastructure

The Preservation of National Security, Economic Stability and Society at Large

There are essential physical and electronic systems that are required for any society to operate and prosper. These systems, which range from utilities to telecommunication systems to emergency services, are classified as critical infrastructure. This critical infrastructure may be managed by private businesses, public corporations, or government entities at all levels. Any threat, compromise, or exploitation of this infrastructure could have a devastating impact on national security, economic stability and the public at large, particularly in catastrophic situations. Therefore, securing critical infrastructure is an utmost concern for governments and businesses globally.

In May 2009, a U.S. Department of Transportation report revealed that more than 750 high-risk vulnerabilities were discovered in 70 applications critical to the operation of air traffic control systems. In addition, more than 800 computer-related security incidents were reported in 2008 to the Air Traffic Organization (ATO), the division of the Federal Aviation Administration (FAA) that manages the movement of aircraft through U.S. airspace every day.

In April 2009, an incident was reported that the U.S. electronic grid was breached by foreign spies that enabled the installation of malicious software ("malware") that could be launched and effectively shut down key portions of the U.S. power grid. The growing concerns about cyber espionage follow the discovery of other significant potential vulnerabilities in that sector. Nearly two years have passed since the Department of Homeland Security orchestrated an experimental cyber attack on a generator at the Idaho National Laboratory. In that simulated attack, an electrical power turbine exploded, revealing a serious vulnerability to the nation's electric grid.

These incidents serve as just a few examples of the potential impact an attack could have on critical infrastructure. According to the U.S. Cyber Consequences Unit, an independent research institute, a single rash of cyber attacks on critical infrastructure could cost in excess of $700 billion.

Because of the potential consequences to economic stablility and public safety, governments around the world are adopting Critical Infrastructure Protection (CIP) programs to ensure preparedness and response to serious threats or incidents that involve critical infrastructure. These countries include the United States, Mexico, Brazil, UK, Germany, Australia, India, and Singapore – along with many others across the Americas, Europe, the Middle East and the Asia-Pacific region (see Appendix A).

The requirements for critial infrastructure protection extends beyond governments and includes an array of systems and organizations that operate critical infrastructure such as:

- Electric, gas and oil utilities
- Telecommunications
- Water utilities
- Transportation systems including aviation, ports, and railways
- Financial services
- Healthcare systems
- Public safety
- Agriculture and food supply
- Information technology

Protecting Critical Infrastructure

As cyber threats become more pervasive, governments and organizations that operate critical infrastructure systems must take steps to ensure that these systems are secure. RSA, the Security Division of EMC, offers a comprehensive set of products and services to help governments and organizations develop a comprehensive CIP program and protect the critical infrastructure systems that are vital to the functioning of our society.

Specifically, RSA can help governments and organizations to:

- Identify key assets that are part of a CIP program and warrant additional risk assessment
- Understand where key assets exist across the infrastructure and evaluate the risks associated with those assets
- Implement flexible security controls to mitigate critical vulnerabilities
- Identify and respond to cyber attacks quickly
- Develop an ongoing and sustainable program for securing critical infrastructure and the systems and data that support them

According to the U.S. Cyber Consequences Unit, an independent research institute, a single rash of cyber attacks on critical infrastructure could cost in excess of $700 billion.

Identify Key Assets and Evaluate Risk

It is impossible to protect key assets if there is no insight into where they exist across the IT infrastructure and in what form. Therefore, the first step in securing critical infrastructure is to identify the location of sensitive data and key assets and determine which of those assets are most sensitive or at highest risk to be targeted. By discovering sensitive data and key assets and classifying them according to their risk level, organizations can begin to define the appropriate usage and handling rules based on industry regulations and sensitivity of the asset. Usage and handling rules may include actions such as alerting, quarantine, encryption or blocking.

There are three key questions that an organization must answer before they can start the process of securing the infrastructure they operate:

- What sensitive data exists within the IT infrastructure and where does it reside?
- What is the value of the data to my organization and the overall operation of critical infrastructure?
- What are the vulnerabilities and/or risks posed to this data?

Once these questions are answered, organizations can start to take the appropriate steps necessary to secure their key assets.

RSA Professional Services provides organizations concerned about protecting critical infrastructure systems with the ability to understand where sensitive data – including incident response plans, disaster recovery plans, source code and other key assets – reside across the infrastructure, and gives these organizations the ability to evaluate existing processes in order to understand how such data arrived there in the first place. With this insight, organizations can take steps to ensure that key vulnerabilities are patched and reduce the risks to sensitive data.

For discovery, the RSA® Data Loss Prevention RiskAdvisor Service offers a full understanding of where sensitive data exists across the organization so that it can be consistently managed and protected. To achieve this, RSA Professional Services leverages the RSA® Data Loss Prevention (DLP) Suite for automated discovery of sensitive data and provides a snapshot of potential exposure. The RiskAdvisor Service encompasses a high-level mapping of business processes and functions to sensitive data to help organizations realize their potential risks.

RSA provides a final report which summarizes the list of machines scanned, a list of files found containing sensitive data, and a profile of the incidence of that data within those files. It also includes a series of recommendations on how to optimize processes to protect sensitive data and establish a foundation for a complete data loss prevention strategy.

Once the discovery phase is complete, organizations must understand the risks presented to their sensitive data and key assets. How could sensitive data and key assets be compromised or stolen? By whom? And what would be the effect on critical infrastructure? Organizations must look internally (employees) and externally (cybercriminals) to answer these questions. Creating a risk model that takes into account all the potential ways data and key assets might be lost or stolen provides the context needed to then help organizations implement the appropriate security controls to protect them.

The RSA Data Loss Prevention Suite offers a comprehensive data loss prevention solution that discovers, monitors and protects sensitive data whether at rest in a data center, in motion over the network, or in use on a laptop, desktop or mobile device. The RSA DLP Suite provides a policy-based approach to securing sensitive data, enabling organizations to discover and classify their sensitive data, enforce appropriate controls, and report and audit, as required.

The RSA DLP Suite offers a robust policy library containing more than 150 “out-of-the-box” policies. RSA boasts the broadest set of U.S. and international policies covering a wide range of regulations, including those targeted at protecting critical infrastructure such as the North American Reliability Corporation (NERC) standards. In addition, the RSA DLP Suite offers a number of pre-built classification modules designed to detect sensitive data related to the operation of critical infrastructure such as disaster recovery and incident response plans.

The policy library is continually being developed and updated by RSA’s Information Policy and Classification Research team, a group of researchers dedicated to studying the U.S. and international regulatory environment and emerging standards and applying that knowledge to develop relevant policy templates that can be applied across multiple industries and regulations.

The RSA DLP Suite also provides superior data detection accuracy by leveraging both fingerprinting and described content detection capabilities, depending on the type of sensitive data and where it resides. Fingerprinting is used for identifying whole or partial sec¬tions of documents and is ideal for data such as floor plans or network diagrams that can be clearly distinguished ahead of time. Described content detection is used for detecting specific types of data, such as credit card numbers or proper names, and is designed to be leveraged across multiple policies.

The RSA Data Loss Prevention Suite is offered in three distinct modules:

- RSA® Data Loss Prevention Datacenter identifies sensitive data stored across file shares, SAN/NAS, databases, and other data repositories such as content management systems.
- RSA® Data Loss Prevention Network identifies sensitive data as it is transmitted throughout the network and enables polices to be enforced across areas such as corporate email systems, web-based email systems, instant messaging, and web-based protocols.
- RSA® Data Loss Prevention Endpoint identifies and controls sensitive data on endpoints such as laptops, desktops and mobile devices.

Implement Flexible Security Controls

Not every key asset will be of equal importance from a risk management perspective. Once an organization has discovered the sensitive data most relevant to the protection of critical infrastructure and has gained insight into the origin and nature of the risks against it, the next step is to implement security controls in order to mitigate critical vulnerabilities. Organizations should enact a combination of data and access controls to:

- Prevent malicious or accidental leakage of critical information
- Enforce rights management on key documents within the critical infrastructure
- Secure access to critical assets and repositories that contain critical assets

Prevent inappropriate distribution or leakage

Organizations must be able to control the movement and usage of sensitive data to prevent inappropriate distribution or leakage. There are two key threats that critical infrastructure providers must address. First, there is the threat from employees of leaking sensitive data, whether the action is inadvertent or done with malicious intent. For example, this could be an accidental leakage based on a lack of knowledge surrounding security policies or the result of a disgruntled employee seeking to cause harm.

Second, there is the threat of malicious software ("malware") being installed on the network and pervading throughout the IT infrastructure. The malware developed by cybercriminals today is very advanced and is constantly being updated through command and control (C&C) servers, rendering it capable of bypassing many anti-virus systems.

This is a very real and growing threat facing governments and private organizations, as well. A successful malware installation can perform a number of seemingly dangerous tasks, including capturing login credentials of administrators or automatically sending out sensitive data that may be critical to operations.

Identity awareness capabilities are critical when implementing data controls. Organizations must be able to determine the individuals or groups that can access and use sensitive data, and establish controls to make sure the data is being handled properly. This ensures that the right data is allowed into the hands of the right users and that the proper notifications and controls are in place to prevent inappropriate handling or misuse. Identity awareness includes:

- Identity-based policy involves establishing policies as to how sensitive data should be handled based on the user or group.
- Identity-based notification involves notifying the necessary individuals and/or groups to take appropriate actions depending on the severity of the incident.
- Identity-based control involves developing controls based on identity at the individual or group level. Examples of identity-based controls include enterprise rights management and access controls.

Organizations must be able to control the movement and usage of sensitive data to prevent inappropriate distribution or leakage.

The RSA DLP Suite is an identity-aware solution that leverages Microsoft Active Directory® (AD) Groups on the network and at the endpoint to identify which files users are accessing, who gets notified in the event a policy is violated, and how incidents are handled. The RSA DLP Suite enables organizations to:

- Set granular data control policies based on the individual or group
- Implement policy-based remediation actions, such as alerting, blocking or encrypting, based on individual or group identities for data in use or data in motion
- Notify specified users when a policy has been violated

The RSA DLP Suite also offers a self-remediation option so a user can be personally notified when a policy is violated and allowed to make a decision about what action to take. This option is good for raising education among employees concerning how their actions can put data at risk.

Enforce rights management

The RSA DLP Suite has been integrated into the Microsoft Rights Management Service® (RMS) platform to discover and automatically protect sensitive data at rest. This reduces the risk of data owners failing to apply the proper policy-based remediation actions, and it protects the most important data by applying RMS controls based on data sensitivity. This results in protection based on content and identity awareness which further reduces the risk of data loss.

Secure access to key assets

Upon applying the necessary data controls, it is important for organizations to implement strong authentication to secure access to sensitive data. While data controls may be in place to minimize the risk of data loss, if the user that gains access to that data is not who he or she claims to be, it can still be handled inappropriately. There are several factors to consider in determining what type of authentication to apply including:

- **The value of the data.** The higher the value of the data is and the higher the risk to an organization if the data is accessed by an unauthorized user, the stronger the authentication mechanism that is needed to protect it.
- **Planned usage.** Who is the user(s), what types of data will they be accessing and what activities do they perform.
- **Technical environment.** If a user is accessing sensitive data remotely or from a mobile device, organizations may determine additional authentication layers are necessary.

Online criminals frequently reuse the same infrastructure to launch attacks. For example, access may be attempted from a common series of IP addresses. However, cybercriminals are developing more sophisticated techniques, such as the use of fast-flux networks, to hide the true origin of the infrastructure being used to penetrate systems. Fast-flux is an advanced DNS technique that utilizes a network of compromised computers that enables a constant rotation of IP addresses, and thus makes the source of the attack harder to detect.

The RSA eFraudNetwork™ service is a cross-organization online network that tracks the patterns and profiles used by online criminals across more than 140 countries. When a potential attack is identified or suspected, the data is moved to a shared centralized repository and then disseminated to members in real-time. The information contained within the eFraudNetwork service can help ensure that known or suspected infrastructure used by online criminals is not leveraged to attack critical infrastructure networks.

Organizations require real-time tracking and correlation of security events in order to respond quickly to potential attacks.

RSA offers a number of choices for strong authentication so organizations can ensure that critical infrastructure systems are secured and only accessed by trusted users.

Secure access to high-value assets and administrative consoles that control key infrastructure components

RSA SecurID® authentication

RSA SecurID® two-factor authentication is based on something you know (a password or PIN) and something you have (an authenticator). The authenticator generates a new one-time password (OTP) code every 60 second making it difficult for anyone other than the genuine user to input the correct token code at any given time.

To access resources that are protected by the RSA SecurID system, users simply combine their secret personal identification number (PIN) with the token code that appears on their authenticator display at that particular time. The result is a unique, one-time password that is used to positively assure a user's identity.

RSA SecurID authentication offers a range of hardware and software authenticators to suit a wide variety of organizational and user requirements including:

- Hardware authenticators
- Software authenticators for desktops and mobile devices
- Hybrid authenticators for combined OTP and digital certificate use

Secure access to environments that maintain sensitive data for large user populations

RSA® Adaptive Authentication

RSA® Adaptive Authentication is multi-factor authentication solution that provides strong and convenient authentication to large user populations.

Leveraging risk-based authentication technology, RSA Adaptive Authentication measures over one hundred risk indicators behind-the-scenes to identify high-risk and suspicious activities. Each activity is assigned a risk score based on indicators such as device forensics, user behavioral profiling, and fraud intelligence. With RSA Adaptive Authentication, the majority of users are authenticated with no disruption. A user is only challenged when an activity is identified as high-risk and/or an organizational policy is violated.

RSA SecurID authentication works seamlessly with RSA Adaptive Authentication and serves as an ideal combined solution for users accessing high-value data or as a second form of authentication for challenging high-risk activities.

Identify and Respond to Potential Threats

Organizations require real-time tracking and correlation of security events in order to respond quickly to potential attacks. Security information and event management (SIEM) systems enable organizations to analyze and report on security logs and events occurring across the network. These logs monitor systems and keep a record of security events, information access, and user activities both in real-time and for forensic analysis should a high-risk event or attack occur. And when those attacks are targeted at critical infrastructure, response must be immediate in order to preserve the well-being of society.

While identifying potential attacks is important, a SIEM solution must also have a streamlined incident handling process. For example, if a major system is affected or anomalous activity is detected, it is important that an incident is routed to an administrator in a timely manner and escalated appropriately, depending on the severity of the incident.

SIEM solutions also provide insight into the "health" of network operations through continuous monitoring of network assets, availability and the status of people, hardware and business applications. This is also important to the operation of critical infrastructure because a failed server, for example, could cause a major disruption. When an abnormality is detected, an IT administrator can be alerted to troubleshoot the problem and prevent critical infrastructure from being impacted.

RSA enVision® log management

RSA enVision log management is a solution that turns raw log and event data into actionable information to help organizations identify and respond to high-risk events. With the RSA enVision platform, organizations operating critical infrastructure systems are able to gain a real-time view into their security environment to ensure the systems, and the documents and data within those systems, remain secure.

The RSA enVision platform offers comprehensive correlation, analysis, monitoring and alerting capabilities to make it easy to consolidate and review daily logs from different systems, including logs from all critical intrusion detection, authentication, and authorization protocol servers.

The RSA enVision platform establishes a centralized point for tracking and monitoring access to key assets and systems - from the users that access it to the activities they perform - and if those attempts are valid. It provides a detailed view of the events that trigger security threats, including insight into the patterns forming on the networks and the specific IP addresses, ports, hosts, users and protocols involved in these patterns. It can also detect critical errors on high-priority components and network operational issues (i.e., a drive failure) that could directly interfere with the efficient operation of critical infrastructure.

In the case of a high-risk event, the RSA enVision platform delivers automatic notifications to assigned security personnel in real-time. The integration of RSA enVision technology with the RSA DLP Suite further enhances an organization's ability to respond to incidents by offering insight into the specific information that may have been compromised or subject to unauthorized access. This enables organizations to prioritize remediation efforts based upon their level of severity and the value of the assets put at risk.

RSA enVision log management also provides insight into an organization's most vulnerable assets through a user-friendly dashboard. Leveraging knowledge from a repository derived from the U.S. Department of Homeland Security's National Vulnerability Database, it correlates security events with what is known about an IT asset to identify those assets that are most vulnerable. This enables organizations to apply the appropriate patches to critical infrastructure systems before they are targeted by an attack.

To meet compliance, the RSA enVision platform offers a reporting engine for quick and easy access to and analysis of compliance-sensitive data. Organizations can create custom reports based on their specific compliance requirements using an intuitive wizard interface or choose from more than 1,100 built-in reports covering a range of global regulations and standards specific to the protection of critical infrastructure.

Develop an Ongoing Security Program

Information security must be embraced as a continuous process, not just a one-time event. An organization's data and the use of it is dynamic; it is always changing, taking on new forms and being moved around. In order to be effective, organizations must develop an ongoing security program that includes conducting routine checks to identify sensitive data and where it resides. For example, disaster recovery plans are updated on a continuous basis and distributed throughout the infrastructure. Following the path of data and ensuring the necessary policies are applied to protect it are critical to ongoing success.

Preventing Botnets from Affecting Critical Infrstructure

Researchers recently discovered a botnet that had infected 1.9 million users across the globe, including many government and corporate computers. The malware associated with the botnet was capable of conducting several hostile actions including injecting code. What if such a threat targeted critical infrastructure systems? A botnet is capable of hampering network performance, in general. Consider the effect, however, if malicious code was injected into a system that controlled a power grid, transportation system, or other public service or utility.

To help prevent systems from being compromised, the RSA enVision platform offers a unique correlation rule to detect a botnet in action. After extensive research into the nature and behavior of botnets and possible detection methods, several ways of identifying potential botnet activity through logs were created. The RSA enVision rule studies network behaviors that are indicative of botnet activity including:

- An increase in detected AV activity with special emphasis on viruses that could be used to gain further system access
- Detected modifications to a host file where host lookup requests are rerouted to a different location
- Changes in DNS utilization
- Internet relay chat traffic from internal or external sources
- An increase in outbound SMTP traffic volume
- An increase in outbound SMTP traffic to known blacklisted servers

RSA Professional Services

RSA Professional Services provides the competencies to help organizations build world-class security programs to ensure that sensitive data and key assets are continually monitored in order to reduce the risk of inappropriate handling or leakage. These services include:

- **The RSA Information Security Policy Development** service helps customers define and map policies to best practices, individual business requirements, and appropriate regulations. The result is the creation and implementation of effective data security policies, which helps to establish a consistent and repeatable way to manage information security risk.
- **The RSA Information Security Program Development** service can help critical infrastructure organizations to classify their multiple security risk remediation initiatives into a project-level roadmap that helps meet requirements for regulatory compliance.
- **The RSA Information Risk Assessment** service is a broad-based security posture assessment for information security that is designed to provide a systematic overview of an organization's information security capabilities and prioritized recommendations for risk remediation.
- **The RSA Classification for Information Security** service helps organizations secure large volumes of data through a structured process and protect information according to its business value.

Conclusion

Critical infrastructure is essential to our way of life. From the electricity we use, to the food we eat and water we drink, to the IT infrastructure that we rely on to conduct everyday business, society is dependent on the security and efficient operation of critical infrastructure.

Natural disaster, cybercrime, equipment failure or a terrorist attack are just some of the threats that could have a detrimental effect on critical infrastructure. Governments and organizations must have the processes and technology in place to address all potential hazards. The RSA solution for protecting critical infrastructure ensures that vital services and infrastructure are protected from the threats that could greatly impact the continued progression of societies around the world.

Information security must be embraced as a continuous process, not just a one-time event.

Appendix

Risks and vulnerabilities are pervasive within critical infrastructure systems around the world. It is not a problem that exists solely in one country or one geography, but is relevant to societies around the world. And as economies become global and more nations continue to become part of the technological revolution, societies depend not just on the efficient operation of their critical infrastructure, but that of other countries. That is why so many governments around the globe have already drafted or started to draft the protection of critical infrastructure into their laws. Here is just a sample of these efforts:

Australia

The Cybercrime Act of 2001 gives federal law enforcement agencies the authority to investigate and prosecute groups who use the Internet to plan and launch cyber attacks that interfere with the functioning of the government, the financial sector, and industry.

Brazil

Brazil is currently working on a Cybercrime Bill that would specify a number of specific activities as cybercrime including disruption of public service utilities.

Canada

The Emergency Management Act of 2007 introduces more comprehensive measures that strengthen the federal role in emergency management and critical infrastructure protection.

Germany

In August 2007, Germany amended its penal code to adopt EU Council Framework Decision 2005/222/JHA to address the threat of attacks against information systems, including those which form part of the critical infrastructure of EU Member States.

India

The Information Technology Act of 2000 provides a legal framework for the protection of electronic transmissions.

Japan

The Unauthorized Computer Access Law of 1999 prohibits unauthorized access to computer systems. In addition, the Basic Law on Formation of an Advanced Information and Telecommunication Network Society 2001 assures security and reliability for networks, including those related to critical infrastructure.

Singapore

The Computer Misuse (Amendment) Act of 2003 requires any person or organization to take necessary measures to prevent or counter any threat that may endanger the national security, essential services, defense, or foreign relations of Singapore.

United Kingdom

The UK has enacted a number of laws for the protection of information systems, including those related to the operation of critical infrastructure. Some of these acts include the Data Protection Act of 1998, the Terrorism Act of 2000, and the Police and Justice Act of 2006.