Cisco Systems

THE SELF-DEFENDING NETWORK: ENABLING PROACTIVE COMPLIANCE AND RISK MANAGEMENT IN FINANCIAL INSTITUTIONS

This paper provides thought leadership on how a self-defending network can enable proactive compliance and risk management for a financial institution—incorporating people, processes, technology, and services necessary to protect the institution and its customers from today's evolving real-time threats.

Prepared By:

Rune Olslund
Financial Services Market Manager

Cisco Systems, Inc.

Paul R. Reymann
CEO
ReymannGroup, Inc.

CONTENTS

A NEW ERA OF BANKING EMERGES

The financial services industry is constantly undergoing change—change that affects internal operations as well as how you interact with your customers. In the past, the arrival of the mainframe, then the minicomputer, and finally the personal computer caused similar transformation in the banking industry. E-banking and electronic operations via the Internet have created a new era of banking.

As each new era develops, people, tools, and methods undergo significant change. In short, there is a human side and a technical side to the transformation. New tools and systems inspire humans, those who run the financial institutions and their customers, to explore new boundaries of banking conduct.

In addition, as we become more reliant on this electronic financial exchange, we rely more heavily on the use of technology designed to allow outsiders in, not keep them out, and technology that is designed to allow insiders and customers to more easily gain access to and transfer data. The movement of paper and back-office operations is being replaced with larger, geographically dispersed networks, e-mail, and Web applications; enhanced databases; IP-enabled ATMs; electronic bill payments; contact centers; wired and wireless personal computing devices; and the Internet. Unfortunately, with this evolution, the vulnerability to common network security threats such as worm and virus outbreaks, theft of corporate information, and distributed denial of service (DDoS) attacks is drastically increasing.

New challenges are emerging from complying with regulatory mandates to ensuring your organization is protected against other types of safety or electronic threats. Security threats have evolved with the expansion of our reliance on networked technologies. The response time from discovery of a new threat or vulnerability to identifying the effect on your network has reduced from weeks to hours, and in many instances, seconds. And if that wasn't enough, your customers and employees still want 24-hour availability. They typically have little tolerance for operational disruptions. Evolving threats can seriously affect your network quickly if not detected and addressed as outlined in Figure 1.

Everyone, from the security personnel and lead staff to executive management and board of directors, is increasingly aware of the threats and risks. They are not only concerned about the internal or external disruptions they cause, but the additional responsibilities and costs associated with ensuring compliance with laws and rules while ensuring business continuity and customer trust.

Customer trust is a bank's stock-in-trade; banks play an important role in maintaining public trust and confidence in the U.S. financial system. In the United States, people recognize financial institutions as one of the eight critical infrastructure components that we must protect. The business operations of financial institutions and the industry as a whole must be resilient and fully capable of minimizing disruptions.

"Proactive information security and technology risk management is no longer an industry best practice—it is a legal mandate!"

Paul R. Reymann
CEO
ReymannGroup, Inc.

In today's fast-paced, high-threat, and heavily regulated financial institution environment, traditional reactive security techniques do not provide adequate security. Each financial institution, its customers, and the industry must be protected by a proactive security strategy that establishes a self-defending network.

A PROACTIVE SELF-DEFENDING NETWORK IS NEEDED

A self-defending network can enable proactive compliance and risk management for a financial institution–incorporating people, processes, technology, and services necessary to protect the institution and its customers from today's evolving real-time threats.

Prudent information security and technology risk management are no longer industry best practices—they are legal mandates. Emerging laws and regulations are mandating a heightened awareness and understanding of information technology and security at the chief executive levels of most organizations. Such knowledge is critical to the success of today's companies.

In the past few years, federal and state governments have increasingly enacted laws and rules that expand the technology, information security, internal control, and corporate governance, as well as other risk management responsibilities of financial institutions. Comprising technologies such as virtual private networks (VPNs) and based on industry standards such as IP Security (IPSec), and Secure Sockets Layer (SSL), self-defending networks address many of these crucial risk management mandates as outlined in Figure 2.

The financial services industry has renewed its attention on proactive information security. Whether you have an established information security program or are just beginning to realize the importance of ensuring your financial institution has a safe, sound, and secure infrastructure, today's risk management strategies call for a broad set of layered security solutions that are proactive, not reactive. Such layered solutions typically include people, processes, technology, and tools. All these components must operate together as part of a cohesive security program. The best strategy for protecting against today's real-time dynamic threats includes:

Figure 1
Security Challenges and Concerns—Threat Evolution

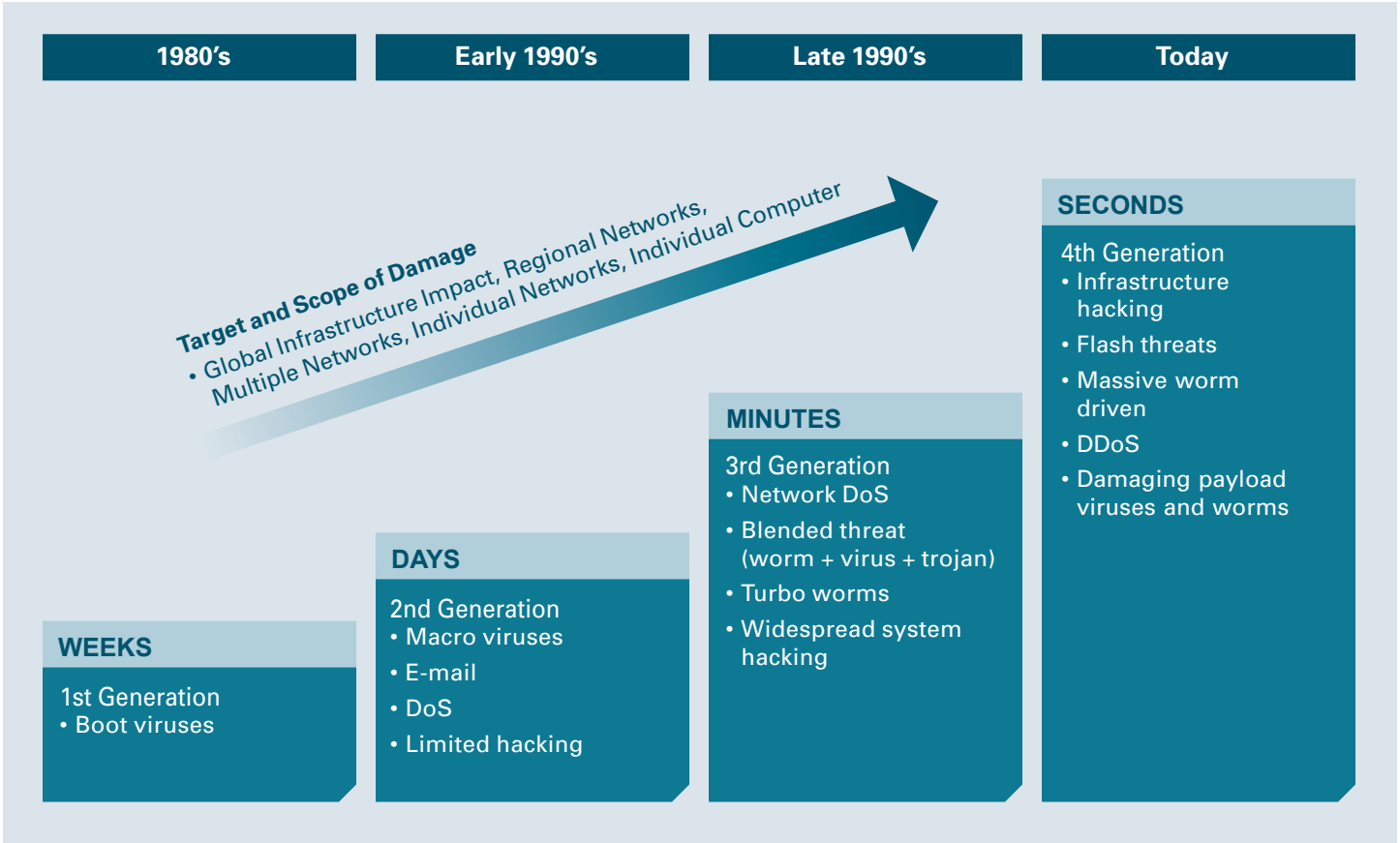


Figure 2
Legal and Regulatory Roadmap to Compliance and Risk Management

Laws & Rules	Risk Management Mandates	Self-Defending Network Enables

Gramm-Leach-Bliley Act Data Protection	• Protect security and confidentiality of customers' non-public personal information
	• Institute administrative, technical, and physical safeguards
	• Protect against anticipated threats and hazards to information security
	• Protect against unauthorized access to or use of information
	• Establish a continuous risk-based information security program with:
	  • Board oversight
	  • Assessment of threats and vulnerabilities
	  • Risk management and controls
	  • Training
	  • Testing
	  • Vendor oversight
	  • Monitoring, auditing, and adjusting
	  • Reporting
		☑ Comprehensive data security
		☑ Proactive and automated identification, prevention, and response to threats
		☑ Integrated security throughout the network from all endpoints
		☑ Coordinated and timely response to threats
		☑ Secure data transfer across non-secure networks such as between branches and contact centers
		☑ Encrypted passwords, one-time passwords, and digital certificates
		☑ Centralized monitoring, management, and control
		☑ Continuous risk assessment with real-time:
		  • Network backup and disaster recovery ability
		  • Network and endpoint patch management
		  • Network operating system, user credential and password policies
		  • General network access and usage policies
		  • Reconfiguration of network resources in response to attack
		  • Integrated security technologies within the network infrastructure: routers, switches, wireless access points, etc
		  • Dedicated security technologies deployed throughout the organization: firewalls, VPNs, anti-virus, intrusion detection and prevention systems (IDS/IPS)
		  • Network hardware and software inventory reports
		  • Network security monitoring with raw data logs
		  • Security threat monitoring logs
		  • Security incident response logs
		  • 24 x 7 x 365 IDS and IPS security response capability

Sarbanes-Oxley Act	• Secure information infrastructure • Monitoring of IT processes and non-public information • Risk assessment of internal controls, technology, and information security • Public-disclosure and rapid reporting of material events	
California Senate Bill 1386	• Disclose any breach of data security • Monitoring and reporting systems to identify security breaches • Encryption of personal data	
BASEL II—Operational Risk	• Board oversight • Monitoring • Controls	
Identity Theft Act Pretext Phone Calling Phishing	• Protect personally identifiable information • Monitor for exposure • Rapid and comprehensive response program • Report suspicious activity	
USA PATRIOT Act	• Risk-based systems and monitoring • Report suspicious activity • Verifying customer identity • Keep good records	

- Automated and proactive security solutions
- Integrated security throughout all devices and applications (e.g., desktops, servers, routers, switches, and wireless access points)
- Centralized monitoring, management, and control
- A coordinated and rapid response to threats

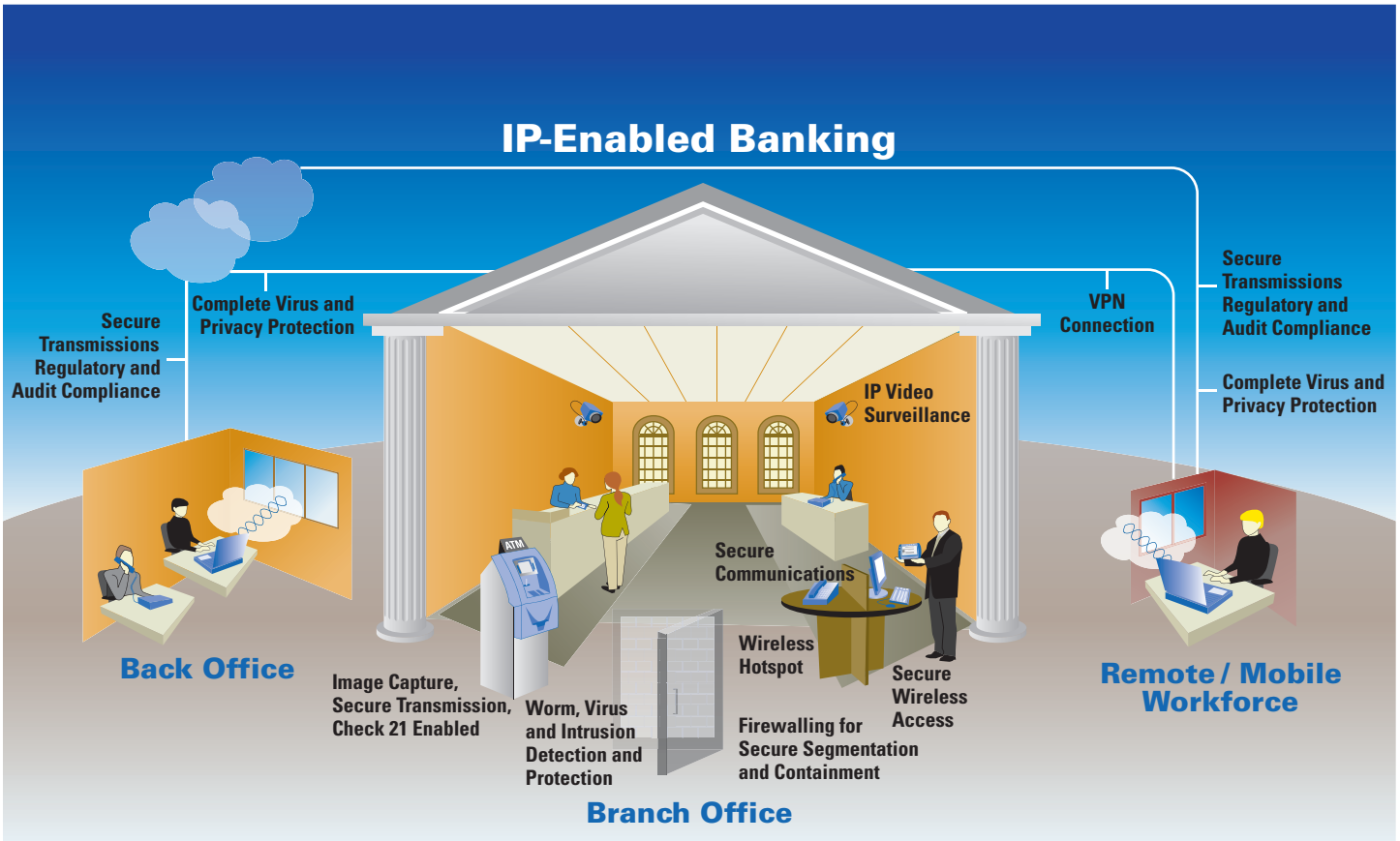
THE CISCO SELF-DEFENDING NETWORK SOLUTION IS THE ANSWER

A Cisco Self-Defending Network based on converged IP technology gives financial institutions the foundation they need to meet their security, legal, and regulatory challenges in guarding against invasions to their networks (Figure 3).

Cisco is the only provider of a "self-aware" network security solution, which consists of three essential components: integrated security, industry collaboration, and a system-level solution to best protect all your critical business resources within your branch offices, back offices, and data centers. The Cisco integrated security solution provides:

- Secure connectivity provides secure transfer of sensitive information across open and untrustworthy networks by using encryption and user authentication to ensure that all communications are secure and private. Collectively, it is comprised of technologies such as VPNs based on industry standards such as IPSec and SSL.
- Threat defense provides comprehensive network security from all endpoints—servers, desktops, and mobile devices. It adds dedicated security to networking devices and appliances, proactively defending the business, applications, users, and network against known and emerging threats from internal and external sources. It consists of security products and technologies such as firewalls, endpoint security software, and IDS/IPS.
- Trust and identity management provides comprehensive network security from all endpoints—servers, desktops, and mobile devices. It adds dedicated security to networking devices and appliances, proactively defending the business, applications, users, and network against known and emerging threats from internal and external sources. It consists of

Figure 3
An Example of a Self-Defending Network for Banks



security products and technologies such as firewalls, endpoint security software, and IDS/IPS.

Industry collaboration combines the best the industry has to offer to detect and enforce system wide security policies. Cisco Systems® works with major antivirus vendors to help ensure that infected devices are not allowed entry into the network. Such collaboration helps ensure that the self-defending network automatically:

- Identifies threats
- Isolates infected servers, desktops, and mobile devices
- Reacts quickly and appropriately to the severity of the threat
- Effectively reconfigures the necessary network resources in response to attacks

A security-aware infrastructure with self-defending capabilities encompasses a departure from individual or point security products and services that operate independently, to a cohesive security system. The network is automated and proactive in defending against threats as they occur with:

- A coordinated and timely response to threats
- Integrated devices deployed throughout the network—such as servers, desktops mobile devices, routers, switches, and wireless access points
- Centralized monitoring, management, and control

Whether your organization is a large or small bank; thrift, savings and loan; credit union; or other financial institution, the Cisco Self-Defending Network can help you proactively and cost-effectively identify, assess, manage, control, monitor, and audit technology and information security risks. As you implement the Cisco Self-Defending Network and align your people, processes, technology, and services to proactively protect your institution and its customers from today's evolving real-time threats, you can achieve:

- ✓ Enhanced security over sensitive data
- ✓ A consistent and integrated security policy across sensitive systems
- ✓ Simplified network management with centralized control and local autonomy
- ✓ A proactive security infrastructure that helps you comply with legal and regulatory audit and examination requirements
- ✓ Enhanced protection against the potential for loss from fraudulent activities such as corporate fraud, identity theft, money laundering, and financial schemes
- ✓ A rapid response for security events to help ensure business continuity
- ✓ Enhanced reputation and customer trust for protecting sensitive information
- ✓ Integration of data, voice, and video applications to improve the customer experience and institution profitability—with contact centers, unified messaging, real-time collaboration, and streamlined security and operations

As a trusted leader in network and endpoint security, Cisco can provide a complete solution that helps mitigate risks and minimize security threats, and that helps financial institutions comply with industry laws, rules, and standards. The cost-effective flexible Cisco Self-Defending Network can be customized to meet the specific needs of each customer; security is tailored to each institution's risk profile.

NEXT STEPS TOWARD PROACTIVE COMPLIANCE AND RISK MANAGEMENT

The first step to a self-defending network includes a careful and complete assessment of your network. The "Network Security Self-Assessment Checklist" included in Figure 4 can help you quickly assess whether you have network security that is proactive, reactive, or open.

The network security practices on the following checklist will help ensure your network is as secure as it can be. It will help you develop proactive, rather than reactive, security and will significantly limit your exposure to threats and the associated liabilities.

Once you complete the self-assessment checklist, contact your Cisco representative or reseller partner or visit www.cisco.com/go/banking to learn more about implementing the Cisco Self-Defending Network in your financial institution.

ABOUT CISCO SYSTEMS, INC.

Cisco was founded in 1984 by a small group of computer scientists from Stanford University. Cisco Systems, Inc. is the worldwide leader in networking for the Internet. Today, networks are an essential part of business, education, government and home communications, and Cisco Internet Protocol (IP)-based networking solutions are the foundation of these networks. Cisco hardware, software, and service offerings are used to create Internet solutions that allow individuals, companies, and countries to increase productivity, improve customer satisfaction and strengthen competitive advantage. The Cisco name has become synonymous with the Internet, as well as with the productivity improvements

that Internet business solutions provide. At Cisco, our vision is to change the way people work, live, play and learn.

ABOUT REYMANNGROUP, INC.

ReymannGroup, Inc. provides finance, healthcare, retail, and manufacturing subject matter expertise. The firm helps companies evaluate their information security infrastructures, determining exposure to vulnerabilities and threats, prioritizing solutions, and complying with legal and regulatory requirements. ReymannGroup provides customers with independent, highly-qualified professionals, authors of regulations, and subject matter experts familiar with financial, healthcare, retail, and manufacturing industry regulations and best practices. For more information, contact ReymannGroup at (410) 286-9505 or info@reymanngroup.com.

Figure 4

Network Security Self-Assessment Checklist

Network Security Guideline—Are you continuously:	Self-Defending Network Enables	Your Network
Conducting network and endpoint security assessments?	✓	☐
Classifying all network and information assets?	✓	☐
Deploying integrated security solutions with intelligent self-defending capabilities?	✓	☐
Identifying areas of regulatory similarities to minimize overhead and avoid duplicate investments in network security? For example, GLBA, USA Patriot Act, and SOX all require consideration of capabilities for: • Firewalls • Encryption • Access Controls • Virtual Private Networks • Intrusion Detection and Prevention • Anti-virus Software • Monitoring, Auditing, and Reporting	✓	☐
Aligning your people, processes, and technology to protect your institution?	✓	☐
Educating each employee on his or her security duties and responsibilities?	✓	☐
Managing security as an essential, dynamic, and ongoing project?	✓	☐
Regularly testing your network and endpoint security to identify weaknesses?	✓	☐
Responding immediately and appropriately to known and unknown, or emerging security threats?	✓	☐
Updating your security practices to comply with new laws, rules, and guidelines and protect against new threats?	✓	☐
Identifying and reporting security-related events to executive management and the board of directors?	✓	☐

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco.com Web site at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in the USA

Job number/productionID/printerID/mo.yr
Lit # XXXXXX