Security and Data Protection

Kamlesh Bajaj
Data Security Council of India

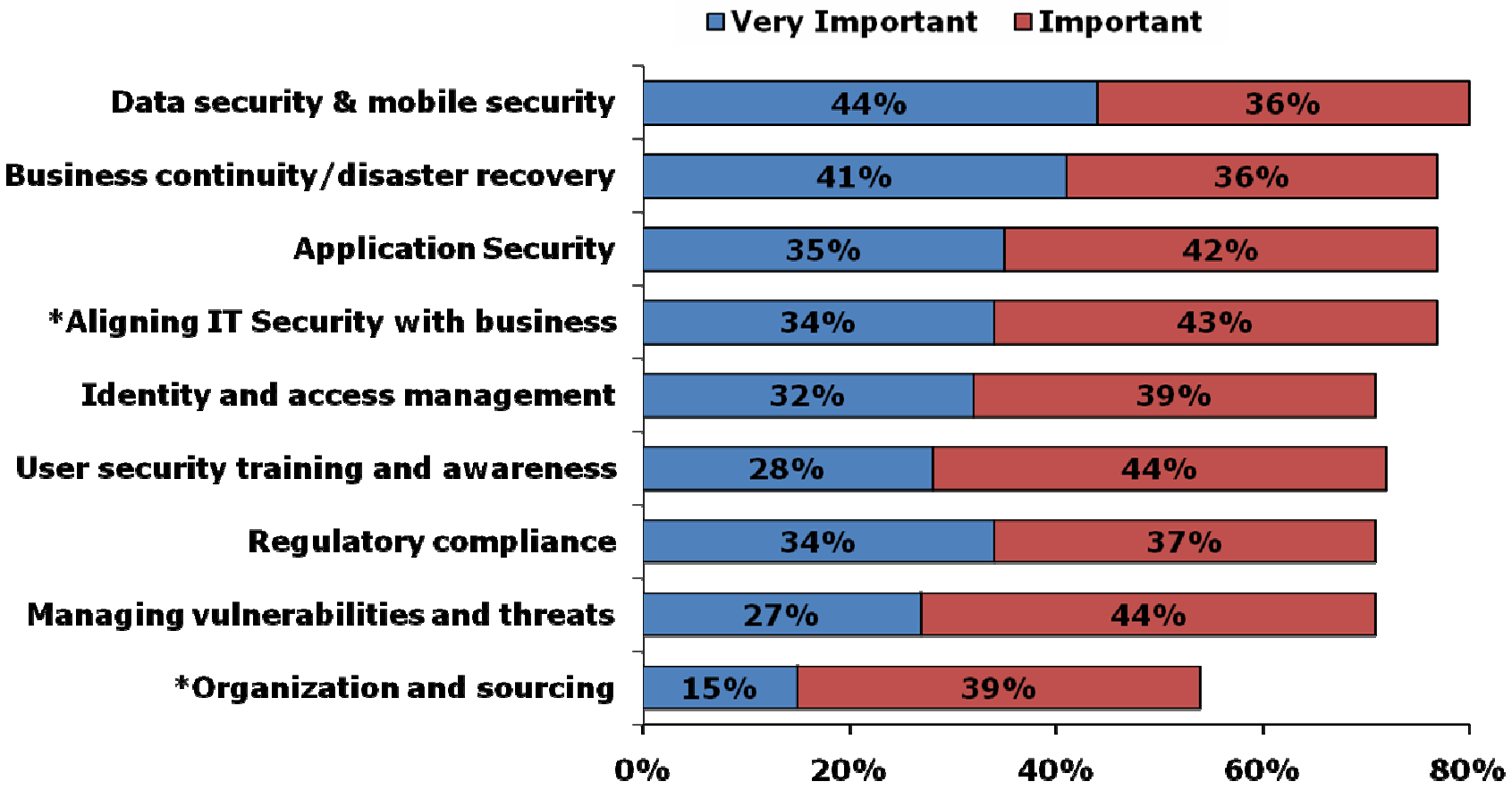
21st August, 2008
OWASP Seminar on Application Security
New Delhi

NASSCOM®
National Association of Software and Service Companies

DSCI | DATA SECURITY COUNCIL OF INDIA

Top Issues: Data Protection Leads, Compliance and Threats Trail

"How important to your IT Security organization will each of the following issues be in the next 12 months?"



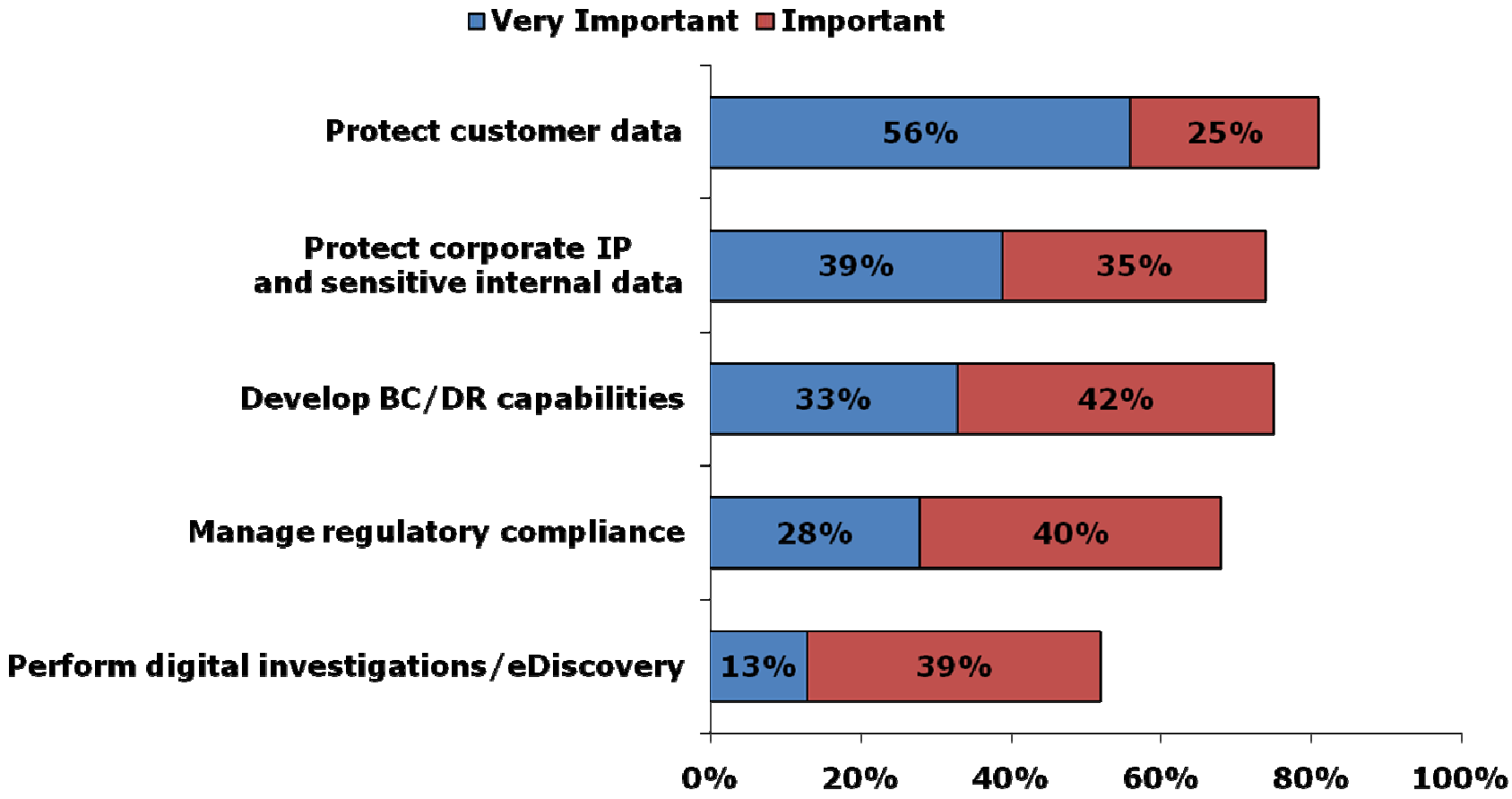
Base: 2212 Security decision-makers at North American and European companies
*1007 Security decision-makers at North American and European enterprises
Source: Security Survey, North America And Europe, Q3 2007

NASSCOM® National Association of Software and Service Companies

DSCI DATA SECURITY COUNCIL OF INDIA

Data Protection is the Leading Business Objective as well

"How important to your IT Security group will each of the following business objectives be in the next 12 months?"



Base: 2212 Security decision-makers at North American and European companies

Source: Security Survey, North America And Europe, Q3 2007

Security Threat Scenario

External Threats

- Viruses, worms, Trojans – malware
- Spyware
- Bots
- Exploit vulnerabilities in platforms, applications
- Launch attacks using unsuspecting users' desktops
- Mail attachments
- Spam
- IRC attacks
- Phishing
- DNS spoofing/poisoning
- DDoS

Internal Threats

- A DBA wiped out critical data after supervisor undermined her authority
- Disgruntlement due to unmet expectations
- Behavioral precursors present, but ignored by organizations
- Insiders create, or use access paths unknown to mgmt to set up their attack and conceal their identity or actions
- Organizations fail to detect precursors
- Lack of physical and electronic access controls facilitate sabotage

Data Scenario & Security Requirements

Data Scenario

- Data on laptops
- Data in files and databases
- Data in Word files
- Data in spreadsheets
- Data sent in emails
- 75 % of all IPRs in emails
- 75 % of all litigation involves some kind of email discovery
- 1 in 50 files contains confidential information
- 1 in 400 emails contains confidential information

Security Requirements

- Perimeter security
- Platform security
- Endpoint security
- Application Security
- Email Security
- Authentication & Authorization for access to data
- Identity protection
- Customer data protection
- IPR Protection

Securing the Enterprise

Information Security – Strategic View

- **Infrastructure Protection**: keep the unauthorized users out – FW, IDS, IPS, AV, SCM, MSS
- **Secure Business Enablement**: let the genuine users in – IAM, strong authentication, access controls, digital rights management
- **Security Administration**: keep the wheels going – security operations, security awareness, information security organization, BCP/DR

Information Security – Operational View

- **Threat Management**
  Perimeter, internal network, applications security; VoIP, Web services, and storage networks, Wireless and mobile security ; Moving from detection to prevention ; Application layer protection
- **Secure Content Management**
  Spam, Spyware, Adware, Web content
- **Security and Vulnerability Management**
  Risk management , Application and software security vulnerability mgmt
- **Identity and Access Management**
  Access control, Identity confirmation, User provisioning
- **Information Security Service**
  Threat focus, Application security, MSS

IS strategic view same as before, but more and more security concerns

Securing the Enterprise

Top Security Concerns

- Security-conscious people, an important layer in defense-in-depth security strategy – awareness programs
- Secure perimeter, weak web apps embed security in app dev
- Mobile technology significant risk
- Identity management and access control need to work in concert
- BCP/DR dev and implementation
- Information Leak Prevention
- Protect Data – secure data rather than infrastructure: data-centric model - define strategy : info classification and data encryption

Security Organization

- Enterprises need structured approach to Governance, Risk, and Compliance (GRC)
- Risk Management Program -> Enterprise Security Strategy -> Enterprise Security Program
- As part of RMP, align security with business – security business enabler
- Use governance framework to facilitate compliance and security
- Focus on security process to achieve maturity, in addition to controls and security architecture
- Define security metrics based on business objectives and security priorities
- Security program maturity takes 5 years of effort: roles & responsibilities, controls, architecture, process maturity, architecture migration
- Outsourcing strategies

Need to protect enterprise information assets throughout lifecycle
Not merely a technology problem - Security culture, awareness, controls, processes

DSCI – Mission

- To create awareness among industry professionals and other stakeholders about security and privacy issues
- To build capacity & provide training among members to develop, & continually improve appropriate data protection & security programs
- To adopt, monitor & enforce an appropriate security & data protection standard for the Indian IT/ITES industry that would be adequate, cost effective, adaptable & comparable with the global standards
- To create a common platform for promoting sharing of knowledge about information security & to foster a community of security professionals & firms
- To provide appropriate oversight and certification services for member organizations

DSCI – Objectives

- Adoption of Best Global Practices
- Independent Oversight
- Self – Regulation
- Focused Mission
- Enforcement Mechanism

Thank You

Kamlesh Bajaj
CEO, DSCI
kamlesh.bajaj@dsci.in