

|N|Y|B|A|

MANAGING EMPLOYEE ACCESS: VPN RISKS, INTERNAL CONTROLS, AND OTHER ISSUES

Lead by:

Joe Compton, President, Core Information Management, Inc.

Harshana Senanayake, Senior Vice President & Chief Information Officer, Northfield Bank

JB Snyder, Principal, Bancsec, Inc.



TERMS

- Risk: the probability that a particular threat will exploit a particular vulnerability
- Safeguard: protective measures implemented to ensure assets are available to meet business requirements
- Threat: an event with the potential to cause unauthorized access, modification, disclosure or destruction of information resources, applications, or systems
- Vulnerability: a weakness in a system, application, infrastructure, control or design flaw that can be exploited to violate system integrity

TERMS CON'T

- VPN: Virtual Private Network utilizes public telecommunications networks to conduct private data communications
- Encryption: is the process of transforming information using an algorithm to make it unreadable to anyone except those possessing special knowledge

EMPLOYEE ACCESS

- **What:** Software Applications, Data, Printers, etc...
- **Where:** Internal workstations, Smart Phones, Laptops, Net books, Web Browsers, Virtual Networks, etc...
- **How:** Policy, Authentication, Encryption,

ACCESS RISKS

- What are they?

ACCESS CONTROLS

- Define User Roles -- Can be as simple as a spreadsheet

User	Core Processing	Teller	Office Applications	E-Mail	Local File Storage
User A	X		X	X	
User B		X		X	

VPN RISKS

- Unauthorized access to the internal Network resources, Data compromise
- Spread of Viruses, Worms and Trojans
- Split Tunneling resulting in an attacker gaining access to a remote computer and thus gaining access to the internal corporate network.
- Use of public machines which may not be patched or have virus scanning software. The same is true for home computers if not patched. This can compromise a SSL session by an attacker using an active session.
- Man in the middle type of attack where user's credentials are captured.

RISK MITIGATION

- Strong user authentication – Multi factor authentication via SSL communications and encryption (DES or 3DES)
- Limiting VPN access to corporate issued Laptops. – With local firewalls and additional digital certificates incorporated
- Operating system and patch level verification at the VPN entry point and when Laptops are returned to the internal LAN
- Policy based controls both at the system level and user level
- End user education to include security awareness and restricting VPN resources based on established corporate high availability requirements consistent with risk tolerance
- Limiting the access to internal resources based on pre established limits