INTERNET SECURITY IN A CHANGING IT ENVIRONMENT

Erich W. Bublitz

Managing Director, One Point Security Solutions

onepoint
Security Solutions
SINGLE POINT OF CONFIDENCE

THE LATEST DEVELOPMENTS IN INTERNET SECURITY

onepoint
Security Solutions
SINGLE POINT OF CONFIDENCE

The Premise

- A new shift is occurring within the technology environment.

- No longer is the IT environment contained within the walls of the organization.

- Two major changes are occurring that are changing the landscape for internet security:
  - Software as a Service (SaaS)
  - Platform Independent Computing

- The focus of internet security has to change to keep pace with the new environment.

Historical Focus of Information Security

- IT originated with a mainframe environment. The focus was security around the mainframe. The only area to guard was the mainframe itself.
  - Strong Passwords and Proper User Rights
- The advent of the client-server environment resulted in a shift in security to focus on not only the server environment, but the protection of the client platform as well.
  - Patch Management and Desktop User Rights
- The propagation of internet connectivity within organizations resulted in the protection of the perimeter. If you could keep the bad out, you could keep the environment safe. This resulted in the candy coating analogy – hard shell with a soft center.
  - Firewalls and External IDS Solutions

Current Focus of Internet Security

•A significant percentage of network attacks are occurring from the inside, employees and contractors.

•Perimeter protection is no longer considered sufficient to protect an organization's valuable information. The analogy has changed from a hard candy shell with a soft center to a hard piece of candy with all layers of the organization being protected.

•The current focus of the security environment is that you must protect all aspects of your IT environment to keep the entire enterprise safe. From your perimeter to your data center to your desktop, the environment must be secure.

The Future of Information Security

•Your information systems environment no longer stops at your internet perimeter.

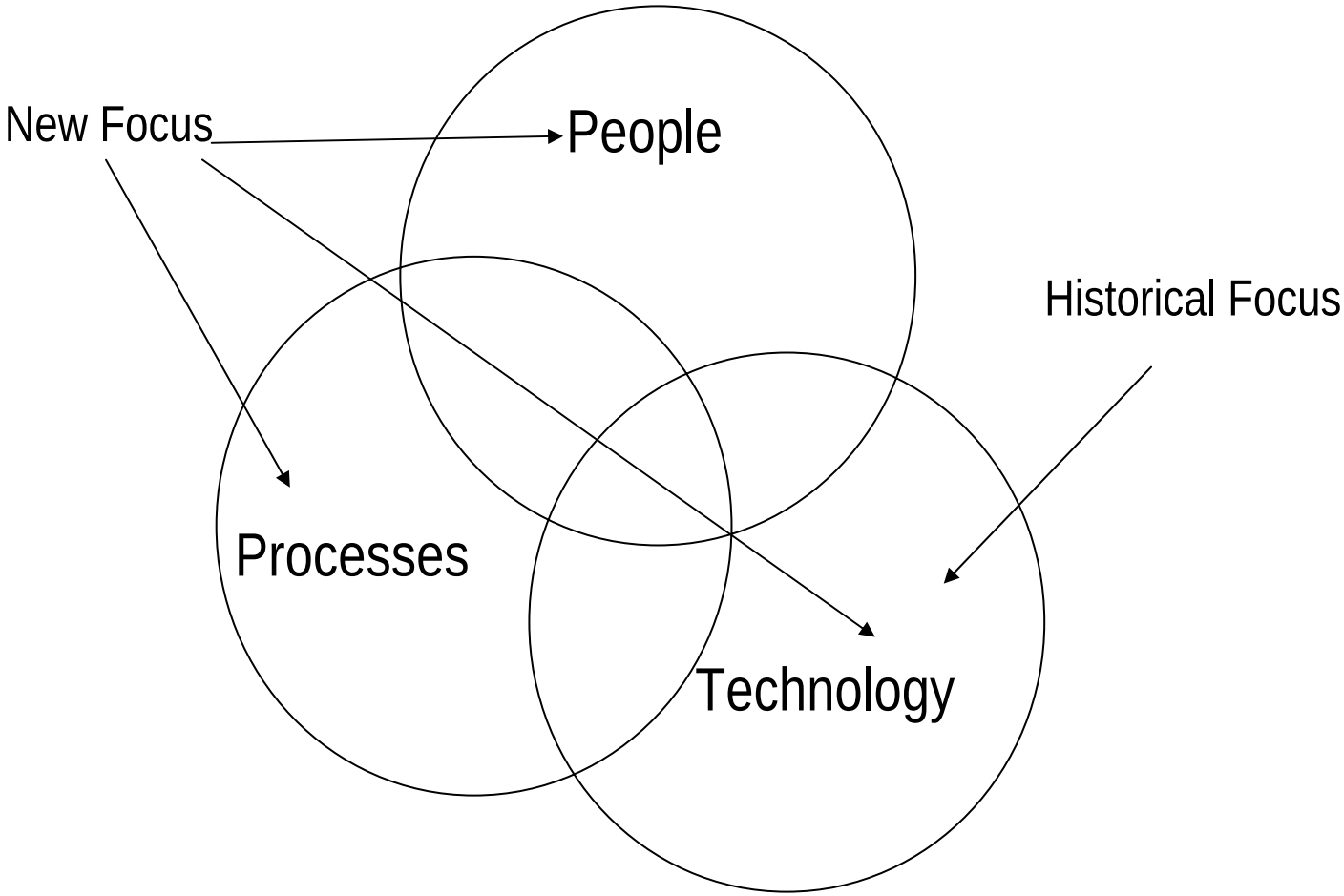
•More and more business is being conducted remotely, using multiple types of platforms, and outside of the confines of the organization's physical environment.

•A fundamental shift in internet security is going to be required to adjust to the new business environment.

THE NEW FOCUS

onepoint
Security Solutions
SINGLE POINT OF CONFIDENCE

The New Focus



What Is Required

A Comprehensive Information Security Program designed to:

- Ensure the *security* and *confidentiality* of customer information;
- Protect against any *anticipated* threats a hazards to the *security or integrity* of such information; and
- Protect against *unauthorized access to or use* of such information that could result in substantial harm or *inconvenience* to any customer or user.

New Technological Focus

- The platform is becoming irrelevant.

- The newer generation entering the workforce is no longer willing to accept the previous paradigm that the organization provides the platform. They want to perform work on a platform of their choosing. Some may use Mac, others Windows, and yet others Blackberries.

- No longer can the protection of the information be based on a protection of the platform, it must be based on the protection at the source of the information.

- The firewall is no longer used to keep people away from your data as you must place it on the public internet.

New Areas To Consider – Mobile Technology

- Mobile Technologies
  - Mobile computing historically was a luxury for organizations, limited to few users. That no longer is the case and is considered a requirement for many organizations at all employee levels.
  - Access to information is required on a multitude of platforms from the phone-based device such as a PDA to a laptop. A new breed of technology is filling the gap between the PDA and the laptop, the ultraportable.

Mobile Technology Security

•As the use of mobile technology continues to become mainstream, the protection of information on the mobile devices must become paramount when designing your information security program.

•Some of the requirements when designing a mobile technology security program include the following:

- •Securing the information from source to destination.
- •Limiting the data that is stored on the mobile device.
- •Knowing who has mobile devices and what information is stored on the devices.
- •Protecting the information when the mobile device is lost or stolen.
- •Protecting the information when an unintended user is accessing the mobile device (a spouse, child, friend, etc).

New Areas to Consider – Application Protection

•Historically, web-based applications contained a limited subset of the information your organization maintained. Now and in the future, the core business applications are being placed on the internet.

•While previously you had a layer of protection by preventing unauthorized users from accessing the application at all, that layer of protection is being dissolved within the new structure.

•The application must securely present the data to intended users. This requires that authorization controls, authentication controls, and application security controls must all be in place.

Web Application Security

•Application security has primarily focused on the appropriate use of user authentication and authorization. Little to no focus is applied to the application vulnerabilities.

•According to the latest Symantec Global Internet Security Threat Report, nearly 70% of new vulnerabilities are designed to take advantage of flaws in web-based applications and browsers. Eighty percent of those vulnerabilities are easily exploitable.

•Developers focus on functionality and deadlines – not securing applications.

•People generally assume that SSL provides security to web applications, it really just encrypts attackers' activity.

Web Application Security – Attack Goals

Attack Goal	Percentage
Stealing Sensitive Information	42%
Defacement	23%
Planting Malware	15%
Unknown Attack	8%
Deceit	3%
Blackmail	3%
Link Spam	3%
Worms	1%
Phishing	1%
Information Warfare	1%

Web Application Security – How

Attack Used	Percentage
SQL Injections	20%
Unintentional Information Disclosure	17%
Known Vulnerability	15%
Cross Site Scripting	12%
Insufficient Access Controls	10%
Credential / Session Prediction	8%
OS Commanding	3%
Misconfiguration	3%
Insufficient Antiautomation	3%
Denial of Service	3%
Redirection	2%
Insufficient Session Expiration	2%
Cross Site Request Forgery	2%

Web Application Security – Who

Industry	Percentage
Government Agencies and Departments	16%
Education	15%
Retail	12%
Media	12%
Service Providers	8%
Security & Law Enforcement	8%
Internet	8%
Technology	5%
Politics	5%
Finance	5%
Sports	3%
Health	3%

The greatest number of attacks occur on Government (29%)

Security Through People

•Most organizations believe that information security is obtained through technological solutions.

•An organization's people are able to overcome almost any technology security solution.

•Most security programs are meant to keep outsiders out, but do not cover employee's responsibilities.

•While the people aspect of security is an organization-wide responsibility, the IT function is going to be necessary to help the business develop a comprehensive program including people.

Security Through Process

•Frequent security problems occur due to the lack of consistent and well documented processes.

•Most IT functions are overworked with the mandate to make it work regardless of other areas of concern such as security.

•Creating formalized processes for the IT function and for users when interacting with the IT environment decrease the risk of security breach due to mistake or misunderstanding.

•Processes should be approved by management, but driven by the information technology function.