E

WIPO-ESCWA/EC/BEY/03/5.C
ORIGINAL: English
DATE: April 2003

THE LEBANESE REPUBLIC

UNITED NATIONS ECONOMIC
AND SOCIAL COMMISSION FOR
WESTERN ASIA (ESCWA)

WORLD INTELLECTUAL
PROPERTY ORGANIZATION

WIPO-ESCWA ARAB REGIONAL CONFERENCE ON INTELLECTUAL PROPERTY AND ELECTRONIC COMMERCE

organized by
the World Intellectual Property Organization (WIPO)
and
the United Nations Economic and Social Commission for Western Asia (ESCWA)

in cooperation with
the Ministry of Economy and Trade

Beirut, May 7 and 8, 2003

SECURITY AND PRIVACY ON THE INTERNET

Presentation prepared by Mr. Hazem Malhas, Chief Executive Officer, AREGON, Amman

NEW APPROACHES TO SECURITY

Introduction

The Internet has revolutionized business, but with any revolution comes new risks. Nothing is impenetrable; it is no longer enough to deploy security systems and hope for the best. It requires a new way of thinking and a new approach…

Companies have no choice but to connect their networks to the rest of the world; to link with customers, suppliers, partners, and their own employees. But with that connection comes new threats. Network predators regularly steal corporate assets and intellectual property, cause service breaks and system failures, sully corporate brands, and frighten customers. Unless companies can successfully navigate around them, they will not be able to unlock their full business potential.

We in the region have an uphill battle. Computer infrastructure systems and processes have not been in place for the same length of time that it has in the west so we lack the experience of it they have. We do have an advantage though, the infrastructure is new here and therefore we don’t have issues with legacy systems to deal with.

Before we delve into the subject, it is important to mention that security is distinct from its close cousin privacy. Privacy deals with the degree of control that an organization has over information about it self. Security deals with vulnerability of unauthorized access to this information.

Furthermore, this distinction needs to be made in relations to today’s litigious world. Most e-businesses are investor driven. If the gap between investor expectations and the business reality is large, and if the firm has not exercised due diligence in protecting its information assets, it will encounter corporate and possibly personal liability.

The Threat

There are several types of threats that are prevalent in the Internet world. The main ones are viruses and worms, denial of service attacks and hacking attempts.

Viruses and worms, according to a recent annual study by the Computer Security Institute (CSI) and the FBI, comprised 85% of the security attacks and abuses faced by companies and government organizations. These attacks could lead to major disruptions within an organization, such as network shutdowns and systems failures. This can be prevented by the use of competent antiviral and content filtering software that can detect and block possible virus and worms.

As for denial of service, or DOS, attacks, these are dedicated to the disruption of the commercial activities of the companies by overloading any security measures that the company has in place and causing their shutdown. Once shutdown, no transaction will be able to take place. To prevent DOS or Distributed DOS attacks from shutting down your systems, adequate monitoring for the security systems must be in place to allow actions to be taken in short periods of time.

Finally, hacking attempts, which don’t have to necessarily be from the outside of the organization tend to be the costliest of the security attacks in terms of lost revenue. The majority of theses attempts are to gain access to corporate or customer information. These can be performed by former or disgruntled employees, hackers, criminal groups or even by competing corporations. To prevent these attempts, a complete security infrastructure has to be in place ranging from a security system and 24/7 monitoring to strict polices and procedures.

These Threats once realized, cost organizations a large amount of money not just due to suspension of commercial activity but also the downtime for the back office operations of the organization.

The Message is three-fold

1. Approach security from a management perspective:

Why? Because it is not based on technical matters but on financial constraints, rules and polices, and business strategies. Let’s take a closer look at each of these.

When addressing financial constraints, one needs to balance cost and benefit.

You will see that achieving complete security becomes cost prohibitive since it will cost a huge amount of money for minor increments in the level of security. For example, if you start with a basic level of security, such as firewalls or security gateways, which is achievable for a cost, you will have a level of security that may prevent 95% of major security hazards. To increase the level you would look into upgrading your firewall systems and adding 24/7 monitoring of theses systems, which may increase your security level to 99%. From this point on, the costs begin to geometrically increase as the percentage increases. To achieve 99.9%, you would place Intrusion detection systems. To increase on this level, you would place 24/7 monitoring on these systems, and so forth.

A strong business case needs to be made for significant investments in security. There is a systematic way of approaching this:

> You need to identify information assets based on a specific combination, such as specific databases, files or transactions.
>
> Identify the financial consequences of these information assets that might be compromised.
>
> Identify the costs of implementing control measures that are being proposed to increase security.
>
> Estimate the risks based on the likelihood of compromise.
>
> Estimate the benefits of the proposed security enhancements
>
> Compare the estimated benefits with the costs of implementing the control measures thereby giving you baseline for your costs.

Turning to rules and policies, management *must* enforce the policies and procedures that are set in place by the technical teams or at least set guidelines for the technical teams when theses policies are set up. It is very common for technical departments to setup policies and procedures and then have these policies and procedures not enforced due to lack of management sponsorship.

Rules and policies lead to controls that, once implemented, will give you a well governed and air tight organization medium. Now when we say controls, what exactly are we talking about? There are several controls that an organization can implement. The more controls introduced, the more protected your organization is.

Physical controls: protect and track your software, your hardware and your facilities. For one reason or another, not many organizations keep track of their physical information system assets. This is especially distressing in an age where we are no longer bound by the sheer size of room-size machines that used to house our critical data. Powerful and inexpensive desktops, laptops, mobile phones and PDAs have supported, if not pushed organizations to scatter proprietary information outside the boundaries of the company office, making it more important then ever to track and protect each of these containers. Take a moment and imagine the implications of a lost laptop containing sensitive data.
Go that extra mile; opt for the fire suppressant system to protect your servers, install the advanced security mechanisms in your data center.

Content controls: Identify and determine the security rating of business content. One of the threats I defined earlier is hacking. Recall that hacking does not necessarily originate from outside your organization therefore it is crucial that you control access to the various information fragments of your business. The critical driving factor of data control is the set of rules and policies that is drawn out by senior management.

Implementation controls: set up proper and well-positioned check points to control information system rollouts within your organization. This applies to both home-grown and third party applications deployed. In-house development efforts require particular attention. Segregation of your development and testing team, code reviews, and security interviews prior to roll-outs are some implementation controls that should be in place.

Operations controls: apply strict best-of-practice procedures to protect against accidental or intentional attempts to inflict harm on your software, your hardware, and your content. Install and automate monitoring systems across your network and hardware infrastructure. Setup automatic virus definition updates. Build a disaster recovery plan. These are all examples of operations controls.

Finally, business strategies. These include asset identification and risk management. Management needs to advise on the business strategies early on and discuss the possibilities of these strategies with their technical teams so that the correct infrastructure is built to accommodate these strategies. It may be common that a business decision is based on business strategies but when the implementation is done, it leaves large holes in the security net due to new architecture.

Asset identification: The process of asset identification allows senior managers, key users, and systems administrators to develop an understanding of the information that is critical to a firm and the systems that contain the information. It requires the management team to identify their information assets and the importance of attributes such as confidentiality, integrity, and availability. This process flows from the understanding that not all information should be protected at the same level and that some information and systems are so critical that their loss would have a negative impact on the continuity of the firm.

Risk Assessment: Given the current uncertain economic climate and the difficult technology spending market, it would be almost justifiable not to take the time to assess your organization's vulnerability to the vast threats of the cyber world, however consider this: on average your network will be subject to an attack at least thirty times per week.

The nature and degree of threats faced by organizations is vast and furious. A risk assessment of the likelihood that security will be compromised is essential. Compromised security is not only limited to theft and criminal corruption of data, but to incidental loss of information or the inability to sustain business services for the customer.

Weaknesses in a firm's critical infrastructure, organization and technology all pose potentially immediate risk. Vulnerabilities need to be identified and assessed as part of a security planning exercise.

2. Approach COMPLETE security as an impossibility:

You *can* achieve security by isolating yourself completely but that would make business nearly impossible. That is why you need to select the level of security that you need based on the analyses prepared previously.

Previously, I mentioned, that to produce a cost benefit analysis you need to categorize the information assets that you have and review the security measures for each. Further to that point, you need to also make contingency plans incase of compromise in case for each of these categories. The contingency plans cover recovery, continuity and notification procedures.

Recovery plans detail procedures for restoring data or rolling back to a state before the compromise.

Continuity plans detail procedures for actions that have to be performed when the compromise happens such as warning or notification messages.

Notification plans detail the procedures that have to be performed in case of loss of information assets or their corruption due to a compromise. These cover the legal aspect of a compromise and the requests to the users of the compromised system to re-transact.

All these contingency plans have to be decided upon by the management and not just the technical teams. They would be set as policy and reviewed periodically until the correct frequencies are found.

3. Approach customers' growing awareness of current security issues:

Do not assume that your customers are going to be tolerant of you if you are compromised. Customers today are more aware, they will expect you to be more prepared to handle the eventuality of a security breach or attempt. Management has to decide what is the level of information provided to customers regarding security breaches of even attempts. They also have to be willing to communicate their precautions to customers in clear terms and to warn them in certain cases. These can be set as policies or conditions that are published on the web site before the customer transacts.

Management has to also decide if there is a possibility of providing re-imbursement in case of financial loss to a customer. This can be covered with-in a liability statement or through insurance cover is feasible.

In Conclusion

From what was discussed previously I hope that I have been able to convey to you the importance of looking at security in terms of being driven by people instead of being driven by technology. It is easy to delegate these tasks to the technical teams and forget about them but that will not provide you with the necessary comfort level you need since the matter will be taken care of in only one dimension. Management has to get deeply involved in the security matters since they are the leaders of the organization. They have to be aware of all the aspects that are involved and take a leadership role in setting the guidelines that have to be followed.

Hackers, crackers, bugs, insecure operating systems, along with continual business evolution, will always be present. As a result, new security threats and holes will constantly appear. Today's IT security solutions must be continually improved upon to remain effective and provide business value again tomorrow.

[End of document]