



White Paper

VeriSign Internet Security Education: E-Commerce Survival Training

Contents

I. THE TECHNOLOGY REVOLUTION IS HERE TO STAY.....	1
II. THE INTERNET	1
III. THE INTERNET IS BIG BUSINESS	1
IV. THE NEW ECONOMY.....	2
V. WHERE OLD MEETS NEW	2
VI. FLAWED INFRASTRUCTURE	2
VII. EMERGENCE OF CYBER CRIME.....	3
VIII. OUTSIDE ATTACKS.....	3
IX. INSIDE ATTACKS	4
X. THREATS DUE TO LACK OF SECURITY.....	4
XI. CYBER SECURITY NEED	5
XII. INTERNET SECURITY EDUCATION.....	5
XIII. HOW CAN VERISIGN HELP?	6

I. The Technology Revolution is Here to Stay

If you've gotten as far as opening this document you are undoubtedly aware that the technology revolution is here to stay. In fact, many of the things we take for granted today – email, cell phones, personal digital assistant (PDAs) – were unimaginable for most of us just a few short years ago. This rapid growth of technology, where prices drop while consumer value increases, is historically unprecedented. A frequently asked question is, “How exactly did we get here?”

One of the fundamental enablers of this change, and of the increase in productivity, is the shift to rapid product development cycles – particularly in the case of software. Feature-rich applications that were impossible to develop and deploy in the recent past, are now conceived of and deployed with lightning speed. The increased intensity of business competition has driven this demand for faster and better products made available in the marketplace. In the future the stakes will become even greater, as competition in every sector continues to escalate. Still, entrepreneurs and visionaries will press on in spite of the risks, and deliver new technologies in better ways

II. The Internet

Buying groceries, paying bills, purchasing clothes, seeking medical advice- cyberspace has become a vital part of our daily lives. ITAA, Information Technology Association of America, states that, “Total worldwide Internet users now exceed 300 million...five years from now,...the number of users worldwide will pass the one-billion mark,...”. In fact, the Internet is the most rapidly adopted technology ever – it has taken only 5 years for it to reach 25% of households (versus 35 years for the telephone).

III. The Internet is Big Business

First came the dot com explosion, with most “old economy” companies rushing to put up an electronic retail storefront. This business to consumer (B2C) marketplace quickly mushroomed to billions of dollars in value. Most recently, ferocious competition has made it tougher for “old economy” companies to maintain their advantage. Today, the strategic shift for most companies has been to the business-to-business (B2B) marketplace where companies can partner in a “virtual village” – and thereby increase sales, lower costs, and increase productivity. Instead of just being another sales or communications vehicle to the end consumer, the Internet has become integrated into the

corporate infrastructure. Coinciding with this increased technological integration of the Internet, the value of the average transaction has also increased dramatically.

IV. The New Economy

E-Commerce business is emerging as the “new economy”, which is the increase in productivity made possible by technology that allows us to collect and share more information than ever before.

With more companies running technology-based businesses and connecting systems internally and externally, more sensitive data is now being kept in systems that are available to an increased number of individuals and entities. Underneath everything is the supporting technological infrastructure that makes the “new economy” possible. This infrastructure is made up of legacy systems, client-server systems, and a myriad of new operating systems, applications and devices. The “glue” holding all of these systems together is the skilled knowledge workers, who work harder and faster to produce more.

V. Where Old Meets New

The longer the Internet is around, the more people agree that the perceived distinction between “old economy” and “new economy” is meaningless. In fact, what has been taking place is a melding of business processes and technologies to produce better goods and services. However, the challenge facing most organizations is that integration is rarely an easy thing – particularly when moving at Internet speed. As the Aberdeen Group indicated in a recent white paper, “Despite the best efforts of seasoned IS professionals, enterprises accelerating to Internet speed in the new digital economy will suffer IT mishaps due to the vicious cycle of increasing features, limited resources, and compromised quality objectives”.

VI. Flawed Infrastructure

Certainly, there have been tremendous quality improvements in many areas of systems development and integration. Without these efforts we would not have the widely adopted Internet that exists today. However, that does not mean that responsible IT managers can bury their heads in the sand and assume that existing infrastructure is sufficient to protect the billions of dollars being transacted via e-commerce. Here are a few reasons why we will need to work hard to improve the infrastructure going forward, if we are to have a reliable and trusted “e”-conomy:

- Not enough IT resources available to get the job done well
- Decreased amount of time for product testing and quality assurance
- Security focus is still an afterthought when it comes to product development
- Proliferation and availability of network intrusion (“hacking”) tools

Any threats to these systems would mean costly downtime that can affect our economic health. It is obvious that the survival of this cyber marketplace will depend mainly on safety, security, and trust.

VII. Emergence of Cyber Crime

Unfortunately, not all of us are using the Internet in a positive way. The Internet has not only allowed us to communicate around the world, it has also opened up the doors for electronic crime. The Computer Security Institute's 2000 Computer Crime and Security Survey raised the level of awareness and aided in determining the scope of cyber crime. This survey of large corporations revealed that 70 percent of the respondents detected the unauthorized use of their computer systems in the last year.

During the past few years the most serious financial losses due to attacks have occurred through theft of proprietary information and financial fraud, according to CSI. Sixty-six respondents in CSI's 2000 Computer Crime and Security Survey reported a total loss of \$66,708,000 in theft of proprietary information while 54 respondents reported a total loss of \$55,996,000 in financial fraud. These 2000 totals were higher than the combined totals of the previous 3 years!

The survey also confirmed that the following trends have evolved over the past few years:

- A broad spectrum of attacks has been spotted.
- Cyber attacks are hitting organizations from the inside and outside.
- Huge financial losses are reported due to cyber attacks.
- Information security technologies are not the sole solution to prevent these attacks

VIII. Outside Attacks

Internet users are starting to realize the severity of these attacks. In the past 5 years the CSI has found that people are more aware of attacks happening, rather than being in denial. The follow types of attacks have been recognized in the wide spectrum of cyber crime:

- **Unauthorized Intrusion**

Networks that are not 100% protected are prime targets for external intrusion. Between 150 and 200 Web page hacks occur every week at small Web sites, while on larger sites the magnitude is greater. The New York Times Web site was brought down for 9 hours and then vandalized. Information that is tampered with leads to financial losses, service disruptions for a company's site, and potentially irreparable damage to the corporate brand.

- **Service Denial**

Similar to unauthorized intrusion, malicious denial of service also results in the loss of revenue and reputation. Big name Internet companies such as Hotmail, Yahoo!,

and Amazon.com recently experienced denial-of-service (DoS) attacks. Hotmail's site shut down for 3 consecutive days, not only preventing 4 million users from accessing it, but also scarring the reputation of Hotmail.

- **Malicious Downloads**

The "Email Bomb", including the ILOVEYOU and Melissa viruses, has plagued email addresses. More recently, Microsoft's computer system was hacked by a Trojan horse called QAZ due to a few machines being unprotected. Security experts confirm that "this is all it takes" and are hoping for this to be a lesson for other companies to keep their anti-virus software updated and educate their employees on good security practices.

IX. Inside Attacks

Information Security magazine found that more media attention has been placed on the "sexy cyberattacks" cited above rather than insider attacks. But in reality, more of the widespread attacks are now coming from insiders. CSI confirmed this when it reported that the majority of the attacks in the past year have been from insider abuse and unauthorized access.

And insiders are not just trustworthy employees. Business partners, subsidiaries, and 3rd party suppliers have the same access as traditional employees of a company.

X. Threats Due to Lack of Security

Cybercrime is not the only reason for malicious attacks. Could it be that companies themselves are not taking the necessary preventative measures? Yes, says SANS Institute who has developed three lists of mistakes people make that enable attackers:

End Users: The Five Worst Security Mistakes

1. Opening unsolicited e-mail attachments from untrusted sources
2. Forgetting to install security patches, including ones for Microsoft Office, Microsoft Internet Explorer, and Netscape
3. Downloading screen savers or games from untrusted sources
4. Not creating or testing backups
5. Using a modem while connected through a local area network

Corporate Management: The 7 Top Errors that Lead to Computer Security Vulnerabilities

1. Not providing training to the assigned people who maintain security within the company

2. Only acknowledging physical security issues while neglecting the need to secure information
3. Making a few fixes to security problems and not taking the necessary measures to ensure the problems are fixed
4. Relying mainly on a firewall
5. Failing to realize how much money intellectual property and business reputations are worth
6. Authorizing only short-term fixes so problems re-emerge rapidly
7. Pretending the problem will go away if ignored

IT Professionals: The Ten Worst Security Mistakes

1. Connecting systems to the Internet before hardening them
2. Connecting test systems to the Internet with default accounts/passwords
3. Failing to update systems when security holes are found
4. Using unencrypted protocols for managing systems, routers, firewalls, and PKI
5. Giving users passwords over the phone or changing them when requester is not authenticated
6. Failing to maintain and test backups
7. Running unnecessary services
8. Implementing firewalls with rules that do not prevent dangerous incoming or outgoing traffic
9. Failing to implement or update virus detection software
10. Failing to educate users on what to do when they see a potential security problem

XI. Cyber Security Need

As the Internet expands more and more rapidly, there is a greater and greater need for tighter security measures. A recent survey by ITAA, Information Technology Association of America, found "...cyber security to be the next 'top priority' issue facing the IT industry around the globe".

Likewise, the Carnegie Mellon Institute's Computer Emergency Response Team Coordination Center (CERT/CC) stated that the number of security-related incidents in the 1st & 2nd quarters of 2000 has almost totaled the number in the entire year of 1999. It is obvious that instead of "reacting" to the problem a strategic plan of attack is needed. Education will be the next step.

XII. Internet Security Education

To truly be successful in the digital economy, every company will have to rely on a combination of products, services and training provided by partners. It is too risky and inefficient for any company to supply all of these from internal resources.

Products: Business buyers are now able to choose from a wide selection of competitively manufactured and priced goods. From PCs to routers to firewalls – the options are plentiful.

Services: Ongoing services are critical for companies because they allow them to be current with the latest technologies available in the marketplace. They enable companies to embrace best-of-breed products and to continually gain knowledge. .

Training: Only 39% of IT training is provided by in-house employees - due to rapid changes in technology, organizations must rely on outside expertise. Simply put, if you don't keep your IT employees well trained, your technology becomes quickly outdated. This is particularly true in the area of information security where the tools and techniques change with exceptional frequency. Internet security education is critical to providing the proper deployment of security solutions.

Technology makes it possible, and training makes it happen! Get the answers before you need to start asking the questions!

XIII. How can VeriSign Help?

VeriSign offers the necessary expertise needed for businesses and consumers to survive on the Internet. Our security consultants offer training on numerous security solution topics.

Please see the E-Commerce Security checklist below to determine which solution(s) you need.

E-Commerce Security Challenge	Got It? 0	VeriSign Training Solution
Defining security strategy		Strategic E-Commerce Architecture and Security
Defining security policy		VPN-1/Firewall-1 Management I
Network access control		Complete Check Point VPN-1/Firewall 1
Properly manage domain name servers and network address mapping		Fundamentals of DNS and BIND
Traffic Management/Load Balancing		High Availability Firewall 1 for Nokia
Network Performance/High Availability		High Availability Firewall 1 for Nokia
Assessing Network Vulnerability		Complete Applied Hacking & Countermeasures

Evaluate Intrusion Detection Tools & Techniques		Complete Applied Hacking & Countermeasures
Incident Response Strategy		Complete Applied Hacking & Countermeasures
VPN Strategy, technology choices		Essential VPN Components
Secure Remote User Access		Essential VPN Components VPN Deployments
User authentication strategy		Secure E-Commerce with PKI and Digital Certificates
Device authentication strategy		Secure E-Commerce with PKI and Digital Certificates Essential VPN Components
Certificate Authority & PKI strategy		Secure E-Commerce with PKI and Digital Certificates
Investigating VeriSign OnSite		VeriSign Certified Administrator VeriSign Certified Engineer

Sign up today!

Don't be left in the dark when it comes to Internet security. VeriSign's comprehensive portfolio of Internet security courses provides you with the best possible tools to keep your site secure. An educated user is much more likely to make the right choices.

To register for a course, go to VeriSign's Internet security education site:

<http://www.verisign.com/training/index.html> While you're visiting our site, please take advantage of the valuable resources you'll find such as quizzes and white papers, as well as our promotional offers.



VERISIGN, INC.
1350 CHARLESTON ROAD
MOUNTAIN VIEW, CALIFORNIA 94043
WWW.VERISIGN.COM

©2000 VeriSign, Inc. All rights reserved. VeriSign, the VeriSign logo, The Internet Trust Company, NetSure, and Payflow are trademarks and service marks or registered trademarks and service marks of VeriSign, Inc. All other trademarks belong to their respective owners. 12/00