CERIAS Security Visionary Roundtable

Call to Action

Jointly Sponsored by

Accenture
(formerly known as Andersen Consulting)

and

The Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue University

Copyright © 2001 Accenture. This document may, however, be reproduced and distributed.

CERIAS Security Visionary Roundtable

Copyright © 2001 Accenture. This document may, however, be reproduced and distributed.

CERIAS Security Visionary Roundtable

Security Experts Issue **Call to Action** for More Secure World

Executive Summary

"A more secure future" for business and society is at stake, according to some of the world's top information technology security experts. Extraordinary changes in the way we do business and lead our lives in the ever-connected world of the future will create tremendous security challenges. These challenges will be shaped by many of today's emerging trends: the rapid acceleration of network speed, connectivity and the overall number of devices; the removal of the human element from many everyday transactions; and easier and cheaper collection of public and private information. More than ever before, we will demand security solutions that enable businesses to thrive and private information to be protected. The bottom-line is that "doing security right" requires the greater community of business leaders, technologists, educators and political leaders to look seriously at this Call to Action and to commit resources and energy to help lead us all to a more secure world.

On September 25-26, 2000, fifteen security visionaries met as guests of Accenture in St. Charles, Illinois, to participate in the CERIAS Security Vision Roundtable, jointly sponsored by Accenture and the Purdue University CERIAS (Center for Education and Research in Information Assurance and Security). These invited luminaries included early pioneers in information security and security leaders at some the largest and most influential companies in the world. For two days, the group shared their deepest concerns, perspectives on significant trends affecting security in the future, and views on actions needed to move us towards a more secure world.

Deepest Concerns

In identifying primary concerns, almost everyone put the threat of a major disaster on the list. Will it happen? Will it affect our increasingly fragile infrastructure? Will it cause loss of life? How can the potential situation be averted? Why hasn't it happened already? High on the list was concern about the impact of poor quality software, widely distributed on the Internet, and the high potential for harm when software weaknesses are exploited en masse. The participants also expressed concern that the highly publicized security incidents were keeping us from focusing on really critical areas that address policy, process and people issues, such as personnel security, hiring and termination procedures, assurance technologies, and system safety issues. The experts agreed that businesses are more willing to buy technology solutions, yet they are forgetting to use good business practices to ensure employees act responsibly.

Trends

When they debated significant trends impacting security, the common themes included increased complexity and interconnectivity, device proliferation, a global economy, privacy vs. convenience, and the "always on" aspect of computing. The solutions, interestingly enough, did not focus on finding a "star wars" solution, but emphasized what the participants have been saying for long time, " We have to take the holistic approach and address this from many dimensions-- including policy, business process controls, law, personal behavior and technology." There was general recognition among a group of competing technological viewpoints that the problem of security really is as hard as we all believe it is, there are no silver bullets, and there is a lot that has to be done to address the problem.

Copyright © 2001 Accenture. This document may, however, be reproduced and distributed.

Call to Action
The group agreed that more public debate is needed on the issues surrounding privacy so that organizations and individuals have well understood expectations. We need to improve the quality and assurance of software to eliminate security vulnerabilities. We need to better develop and deploy baseline security best practices and standard security architectures. We must pursue a well-rounded, integrated, and proactive approach that addresses business, social, technical and government problems. We have to recognize that this is, above all, a people problem and we must invest wisely in education and awareness.

The participants shared and absorbed an immense amount of information. This paper captures their input on deepest concerns, emerging trends, and a Call to Action for the next decade. This Call to Action must continue to engage leaders in debating and resolving these issues so we can look forward with optimism to a more secure world.

The following list includes the top ten trends impacting security that the group identified. A summary explanation and detailed description of each trend is provided in the full report.

Top Ten Trends

The EverNet:	Billions of devices proliferate that are always on and always connected.
Virtual Business:	Complex outsourcing relationships extend trust boundaries beyond recognition.
Rules of the Game:	Government regulation increases as lawmakers react to real losses that hurt.
Wild Wild West:	International criminals exploit lack of cooperation and compatibility in international laws.
No More Secrets:	Privacy concerns will continue to compete with convenience and desire for features.
Haste Makes Waste:	"Time to Market" increases pressure to sacrifice security and quality of software.
Talent Wars:	Lack of security skills will compound weaknesses of delivered solutions.
Yours, Mine or Ours:	Identifying intellectual property and information ownership will become key areas of debate.
Web of Trust:	Standard security architectures and improved trust will spur eCommerce growth.
Information Pollution:	Information exploitation becomes more lucrative than hacking.

Copyright © 2001 Accenture. This document may, however, be reproduced and distributed.

CERIAS Security Vision Roundtable

Call to Action

The following is a list of action items viewed as most critical by the group of the visionaries. More explanation for each action item is included in the full report.

Improve Software Quality	Focus on improving the quality and assurance of software. Prevent distribution of weak software with security exposures. Conduct research to find better methods for designing and developing higher quality software.
Invest in Training and Awareness	Develop a sound educational program that focuses on security and ethics. Focus resources throughout the educational spectrum. Teach respect for electronic boundaries. Develop comprehensive curriculum to educate our next generation.
Implement Best Practices	Incorporate baseline safeguards and practices. Use best practices to ensure security is done right in development, implementation, testing, business processes, and consumer practices.
Initiate Public Debate	Initiate public debate on identification, ownership protection, use of personal information, and responsible use of computing.
Advocate Holistic Approach	Advocate and pursue a well-rounded and pro-active approach to the overall problems: business, social, technical, and government.
Package Security Architectures	Encourage packaging of a basic security architectures with standard services that integrate with applications and infrastructure.

Copyright © 2001 Accenture. This document may, however, be reproduced and distributed.

The Visionaries

Rebecca G. Bace

Infidel, Inc.

Ms. Bace is currently President/CEO of Infidel, Inc., a network security consulting practice headquartered in Scotts Valley, California. She is one of the world's leading experts on Intrusion Detection. She spent a dozen years at the National Security Agency, where she led the Computer Misuse and Anomaly Detection (CMAD) Research program from 1989 through 1995. After leaving NSA in 1996, she served as Deputy Security Officer for the Computing, Information, and Communication Division of Los Alamos National Laboratory.

John C. Clark

Accenture

Mr. Clark founded and currently leads Accenture's Global Security Practice. He has more than 12 years of experience consulting on security issues and implementing company-wide security programs. Mr. Clark's current responsibilities include building Accenture's global security capability, development and execution to the firm's security practice business plan, defining security market offerings, creation and oversight of go to market alliances, and oversight of all Accenture research and investments in the security area.

Daniel Deganutti

Avanade

Daniel Deganutti is a Fellow and Security Architect at Avanade, a high-tech systems integrator specializing in the delivery of enterprise systems built upon Microsoft technologies. Daniel is based at Avanade's Paris Development Center. Prior to Avanade, Daniel led the Andersen Consulting European security practice, focusing on the design and deployment of secure solutions for the financial services industry.

Whitfield Diffie

Sun Microsystems

Dr. Diffie who holds the position of Distinguished Engineer at Sun Microsystems, is best known for his 1975 discovery of the concept of public key cryptography, for which he was awarded a Doctorate in Technical Sciences (Honoris Causa) by the Swiss Federal Institute of Technology in 1992. Prior to assuming his present position in 1991, Diffie was Manager of Secure Systems Research for Northern Telecom, functioning as the center of expertise in advanced security technologies throughout the corporation.

Glover T. Ferguson

Accenture

Glover is Chief Scientist for Accenture, leading the firm's global technology research and innovation strategy. Glover also is co-director of Accenture's eCommerce Program, responsible for shaping the firm's strategy for realizing the benefits of eCommerce for its clients and for helping to ensure the firm's leadership position in the new economy.

Copyright © 2001 Accenture. This document may, however, be reproduced and distributed.

Daniel Geer, Sc.D.
@Stake, Inc.
Dan is CTO at @Stake, Inc. Dan was Manager of Systems Development at MIT's Project Athena, the first large yet coherent distributed computing plant out of which came the X Window System, Kerberos, and much of the general organization of enterprise computing we now take for granted. A serial entrepreneur, he also presently serves as President of USENIX, the advanced computing systems association.

Anatole V. Gershman
Accenture
Anatole Gershman is the Director of the Center for Strategic Technology Research (CSTaR) at Accenture. Prior to joining Accenture, Anatole spent over 15 years conducting research and building commercial systems based on Artificial Intelligence and Natural Language processing technology.

Michael J. Jacobs
National Security Agency
Mr. Jacobs is the Deputy Director for Information Systems Security at the United States National Security Agency (NSA). Under his leadership, NSA is implementing an Information Assurance (IA) strategy to protect the Defense Information Infrastructure and, as appropriate, the National Information Infrastructure. During his 37 years of NSA service, Mr. Jacobs has been a leader in Information Systems Security production and control, policy and doctrine, and customer relations.

David A. McGrew, Ph.D.
Cisco Systems, Inc.
Dr. McGrew is a cryptographer at Cisco Systems, Inc., where he develops cryptographic systems and protocols, and represents security issues on the University Research Board. His work includes the design of practical security systems using cryptography, with an emphasis on performance, scalability and deployability.

Fred Piper
University of London
Professor Piper is currently Head of the Mathematics Department at Royal Holloway (University of London) and is Director of the Royal Holloway Information Security Group. Fred has published over 80 research papers, 4 books (2 on cryptography), and is on the editorial boards of two international journals.

John W. Richardson
Intel Corporation
Mr. Richardson directs several teams in the Intel Architecture Labs (IAL) which are addressing emerging security and network service issues of the Internet. His Internet Security team has developed solutions for getting Internet Telephony and Multicast through firewalls, implemented multiple security protocols, and is currently exploring issues surrounding distributed network security.

Copyright © 2001 Accenture. This document may, however, be reproduced and distributed.

Marvin Schaefer

Books with a Past

Marvin Schaefer has been actively involved in computer security since the mid-1960s. In 1968, he was an invited participant in design meetings for the ArpaNet and served on a number of DoD and Intelligence Community security studies. In 1982 he became the first Chief Scientist of the newly-formed DoD Computer Security Evaluation Center at NSA, where he was a principal author of the *Trusted Computer System Evaluation Criteria* (*TCSEC*) and where he formed policy and practice for the emerging National Computer Security Center. He retired from Arca Systems in August, but remains active in information security and continues to serve on the New Security Paradigms Steering Committee.

Howard A. Schmidt

Microsoft Corporation

Howard Schmidt currently is the Corporate Security Officer for Microsoft Corporation, Redmond, WA. Prior to that he was a Supervisory Special Agent, Director of the Air Force Office of Special Investigations, Computer Forensic Lab and Computer Crime and Information Warfare. Professor Schmidt is one of the early pioneers in the field of Computer Forensics and serves as a Distinguished Special Lecturer at the University of New Haven Connecticut. He currently is the International president of the Information Systems Security Association (ISSA).

Eugene H. Spafford, Ph.D.

Purdue University

Professor Spafford is a professor of Computer Sciences and a professor of Philosophy at Purdue University, where he is also director of the Center for Education Research Information Assurance and Security. Among other activities, he is chair of the ACM's U.S. Public Policy Committee, a member of the Board of Directors of the Computing Research Association , and is a member of the US Air Force Scientific Advisory Board. He was the year 2000 recipient of the NIST/NCSC National Computer Systems Security Award, and is a Fellow of the ACM, the AAAS, and the IEEE.

Phil Venables

Phil has over 15 years experience in Information Technology across a range of sectors from petrochemical, defense and financial services and across a range of disciplines from systems development, systems management, network architecture/design, information security and e-commerce infrastructure. Phil was the Global Head of Information Security for the Deutsche Bank Group until early 2000 when he took up the position of Chief Information Security Officer for a major US Investment Bank in New York.

Copyright © 2001 Accenture. This document may, however, be reproduced and distributed.

Perspective on the Future

Whether we notice it or not, more and more aspects of our lives are gradually becoming virtual. A few years ago we started paying bills on-line. Today, we trade and shop on the Internet. Tomorrow will bring truly smart connected appliances: medicine cabinets that will monitor our health and communicate with our doctors and pharmacists, wardrobes that will know what clothing we have, cars that will know their positions and occupants, home entertainment centers that will know all our tastes and habits. All this personal information is increasingly stored, updated and communicated in digital form. In the right hands of our service providers it will bring wonderful conveniences and efficiencies into our lives. In the wrong hands, this information can be used to wreck havoc both financially and socially.

Today, we make sure that the doors of our houses are securely locked. We often use security services to protect our physical selves and our possessions. But are all our virtual doors secure? What can we do to protect them without causing great inconveniences for ourselves? This is not a theoretical threat of interest only to very rich people. Today, one can hire private investigators to dig up all kinds of personal information about a person. This is costly and inconvenient. Tomorrow, almost everything we do will be recorded electronically. With the right tools, this information can be collected and analyzed cheaply and efficiently. Businesses will do it to provide customized services that we demand. Others may use these same tools to commit crimes of fraud, impersonation, theft, vandalism, etc. on a large scale with a push of a button.

The new world and the new economic model of connecting everything electronically, requires us to trust in things we can no longer talk to or touch or see.

Whom do we trust?

We trust electronic systems to recognize what is authorized and unauthorized and to act only upon legitimate requests. We trust software vendors to write programs that work as we expect. We trust our service vendors to implement adequate business process controls that help us define what is authorized. We trust our communications infrastructure and our legal infrastructure to protect us and to respond when something fails. We trust those who have access to our personal data as it is stored and shared in cyberspace, i.e., software developers, commercial enterprises, medical providers, insurance companies, delivery service providers, law enforcement, to know what they are doing and understand the implications of this massive and complicated process.

Can we achieve this seamless economic model? If we can, it is only when organizations and governments can assure us that our trust has been well-placed. It is not sufficient for our trust, though, to be in only one entity. In fact, our greatest need for assurance is in the interaction of businesses and the complex infrastructure that supports these transactions. Where are the potential failures that could erode our trust? Some could be technology failures, but many, if not most , will eventually be recognized as people and process failures.

Some of the potential failures could be in the software, but remember people write software and people test software. The management and delivery of immature and weak software products is a people problem. Software that is designed and developed without adequate security protections, safety assurances, and controls, is a people and process problem. Some of the

Copyright © 2001 Accenture. This document may, however, be reproduced and distributed.

potential failures could be in the process of authorization-, we authorize too much without setting reasonable boundaries. The failure could be our own lack of awareness, in that we trust too much and do not ask for appropriate assurances that our privacy and integrity will be maintained. The failure could be in careless employees who do not follow policies and share or sell confidential information (our medical records, our physical location, etc.) or who modify systems to perform unauthorized activities. The failure could be inadequate laws that do not require businesses to take proper precautions until enough failures and lawsuits motivate businesses to address security more aggressively.

Providing security that enables businesses to thrive and that protects both business assets and personal privacy must be approached multi-dimensionally. It requires good business practices and well-planned policies and procedures for software developers, business managers and customers to follow. It requires public awareness and training to ensure people understand their obligations and their risks. It also requires security technology solutions that we can trust to validate identity, ensure only authorized activity, protect privacy, and provide accountability. Security is complex, because failures can occur in so many different dimensions. We cannot rely only on policies, on laws, on personal behavior, or on technology. We must address each of these facets and understand how they impact each other as we focus on creating a more secure world in this new century.

Copyright © 2001 Accenture. This document may, however, be reproduced and distributed.

Top Ten Trends - Summary

The roundtable participants identified several trends that will impact security in the future. The common themes that emerged have been summarized in this list of top ten trends

The EverNet: **Billions of devices proliferate that are always on and always connected**. Technology, culture and the law are all driving us towards this EverNet with millions, and possibly billions, of nodes always connected and always on. The explosion of new devices increases the complexity of our systems to the point where it is not possible to comprehend all of what we are using. The complexity itself will cause things to happen, power outages, network downtime, market crashes, enabling break-ins, that will catch us unprepared and incapable of identifying the causing factors. In addition, we need to resolve issues of identity and authority when these devices conduct activities for people without human intervention, when no one is around to notice.

Virtual Business: **Complex outsourcing relationships extend trust boundaries beyond recognition.** The scarcity of specialized resources, the complexity of the infrastructure, the desire to transfer liability, and the competitive need to focus on core competency is driving many businesses to look for advantageous outsourcing relationships as the move to eCommerce continues. As companies build relationships with other companies who are also building their own relationships, trust boundaries of corporate systems will be extended without a clear understanding of whom is now trusted. Industry will find it difficult to enforce its own business security policy on a process handled by multiple players.

Rules of the Game: **Government regulation increases as lawmakers react to real losses that hurt**. The EverNet is connecting ideologies, philosophies, economies and goals that have never before been connected or only tenuously connected. These conflicts will result in challenges to local rules, changes in law enforcement, and an emphasis on contract law. Money and economics, plus concern for damage to critical infrastructure information, will drive lawmakers to act. Legislative reaction will drive changes in the law that should be carefully analyzed for unintended consequences.

Wild Wild West: **International criminals exploit lack of cooperation and compatibility in international laws.** As companies become global, they will rely less on ineffective local government when international crime occurs on their networks and systems. Large companies will become their own defensive force, "carry their own guns", or do as businesses did in the Wild Wild West. They will private security services to protect them where the law is inadequate. In addition, international companies will use local laws to their advantage by picking the country whose laws they wish to apply to their business situation.

Copyright © 2001 Accenture. This document may, however, be reproduced and distributed.

No More Secrets: **Privacy concerns will continue to compete with convenience and desire for features.** Concern will grow about how information is collected and used, especially information considered personal and private. Currently, people seem willing to give up some of their privacy to accept a service that improves convenience or has nifty features. There will be growing pressure for accountability, to know who is involved in a business environment, to assign accountability to actions that occur, to meet the needs of law enforcement, tax collection and the national interest. The security challenges will involve creating a secure infrastructure that can both provide accountability and protect privacy at a level that is acceptable to society.

Haste Makes Waste: **"Time to Market" increases pressure to sacrifice security and quality of software.** The pressures to deliver at eSpeed to the market, forces vendors to sacrifice security and quality for functionality and expediency. Weak and buggy software is delivered, and the consumers assume unknown risk when they deploy unsecured software. These problems are compounded when almost everyone uses the same standard software products and tools. The benefits of standardization become liabilities when weaknesses are discovered and exploited en masse in these products. The growing problem is the volume of easy marks that can be targeted by the unskilled using "shrink-wrapped" exploitation scripts posted on the Internet.

Talent Wars: **Lack of security skills will compound weaknesses of delivered solutions.** Demand for deep security skills is high and supply is very low. Contrary to popular opinion, the skill to break into systems is not the same skill required to design secure solutions. eCommerce requires strong ethical qualifications and a huge breadth of security skills to ensure accountability, to develop robust security architectures, and to protect personal and corporate assets. That need is not being met, and the result is too many web-enabled applications with too many easily exposed weaknesses. The drive for short-term solutions and the "first-to-market" is stifling the ability to invest in the future through adequate funding for research and education.

Yours, Mine or Ours: **Identifying intellectual property and information ownership will become key areas of debate.** The explosive growth of electronic-based intellectual property and the easy ability to transform, manipulate and deliver information anywhere, anytime, will force society into heated debates on information ownership and control. There will be additional questions about what type of information we own, e.g., web habits, on-line purchases, medical records, and how we can control that. Intellectual property rights, creative control and privacy will all be challenged in this debate on ownership and control.

Copyright © 2001 Accenture. This document may, however, be reproduced and distributed.

Web of Trust: **Standard security architectures and improved trust will spur eCommerce growth**. Dynamic networks will continually appear and disappear to support temporary coalitions in business, government and the military. The dynamic nature of these networks, connecting mobile and wireless devices as well as remote networks, brings the issue of trust into the spotlight. The future will provide improved technology to enhance trust, including trusted third parties, industry-sponsored accreditation, digital identities, biometrics and smart cards. Standard security architectures will be developed that provide a set of security services like authorization, certificate management, encryption, and intrusion detection. All of these will be necessary to improve security, but none of these will be sufficient in itself.

Information Pollution: **Information exploitation becomes more lucrative than hacking**. People can exploit the speed and replicative nature of the net to manipulate markets and society for economic or political gain. The interconnectedness of everyone and our ability to spread and respond instantaneously to events, knowingly or unknowingly, increases the chance for misinterpretation causing havoc. Information pollution spreads when large databases contain unchecked, inconsistent and often-incorrect data that is shared, processed, and used without careful monitoring. Mistakes are making their way into the global information ocean and we cannot remove them.

Quotes from Trends Discussion

These quotes convey some of the actual conversation from the Roundtable discussion on trends.

EverNet: On the proliferation of devices, "*All of a sudden we're doing a lot of transactions in those sort of environments. So with this situation, we've got a zillion clients out there operating from all these locations all around the world that were not built for security with people who aren't trained in how to secure it now, which becomes a gateway into the goodies within the network.*"

Virtual Business: The outsourcing trend, "*One of the things we're seeing is with this outsourcing, you lose visibility and therefore control over what's really happening. We see it at the network layer where you think you're going to a website, but you get sent off to a mirror or some of the content from a mirror came into a frame from another site. We see it at the business level which is, I think I have an agreement with this supplier to supply something, but he's outsourcing components of it and we build this incredibly complex value chain that we can't even see down.*"

Haste Makes Waste: Creating secure systems, "*There is no economic incentive to take capabilities away from a system just because they're not secure. If the public wants capabilities, or believe they need to have those capabilities, the vendors are going to provide them. That adds complexity to the system, and complexity is hard to do right. Complex systems may fail complexly but penetrations always work simply.*"

Copyright © 2001 Accenture. This document may, however, be reproduced and distributed.

Deepest Concerns

The experts reviewed the history of security and then discussed their deepest concerns. The following captures the most pressing concerns of the participants.

The sheer magnitude of the problem makes it difficult to achieve security now as well as in the future. The difficult challenges include the level of complexity of systems today, the level of interconnectivity that exists, the distribution of identically weak software, the dependence on people to do things when security will never their top priority, the rapidly emerging threats, the challenge of identifying all of the risks, the challenge of making sure all the holes are plugged when it only takes one weakness for the system to be breached, the lack of available skills to secure systems, and a lack of available end-to-end solutions.

It is difficult to determine how much security is enough. One definition of computer security is that, "A computer is secure if you can depend on it and its software to behave as you expect." Given that we are not very good at defining expected behavior, one could argue that our entire foundation for achieving security is shaky. We lack generally accepted industry best practices, risk assessment is challenging to achieve with adequacy, and one man's security is frequently another man's security exposure.

There is a proliferation of connectivity of systems that were never designed to be secure. Networks were never designed to be secure and many of the operating systems and applications that exist today, or are being developed, either possess security holes or do not have the capability of being adequately secured. We are deploying systems with a number of independent and inconsistent elements and attempting to integrate those elements. Our current focus on network intrusion detection and firewalls, while a creative solution to some of our problems, really represent somewhat of an unnatural act.

The very nature of electronic information makes it difficult to protect. Information is easily copied, transported, and does not have a limited lifetime. Information may be easily corrupted or utilized to misrepresent fact. Restricting access to information and protecting it through intellectual property laws is a challenge. There is also a danger that security, once applied, implies legitimacy. There is a potential for this to be abused.

There is a substantial focus on failures of security rather than looking at the big picture. The complexity is such that the population does not understand the issues. There is also a lack of understanding on how to achieve security with much of the current focus being on the "technology silver bullet" or attempts to validate security by having someone trying to break in. The public understanding is that the skill to break a system equals the skill to build a better system – this is false. For example, penetration testing uncovers a small number of weaknesses and is not a substitute for designing and building security into the system from the ground up. We are not focusing enough on people and process related issues.

Copyright © 2001 Accenture. This document may, however, be reproduced and distributed.

There is a risk of a major information security related disaster – either accidental or through cyber terrorism. The Internet distributes the power of "how to make the bomb" – electronically speaking. In the electronic world, the criminal now lives next door to you and the private sector and law enforcement are currently outgunned. A serious security related disaster could have direct impact on the public and could also lead to an over-reaction such as laws and policies that frustrate efficiency and the emergence of new businesses.

Our ability to deploy and manage systems is not keeping up with the threat. We are basing a lot of security on inadequate, and sometimes unproven, technology. Security practices are often rejected by corporations and standards bodies in favor of features and time to market considerations. There are inadequate commercial incentives to comply with any particular security metrics.

- We frequently build systems and applications without adequate quality assurance, testing, and fault tolerance, and are increasingly dependent on this fragile web of interconnected systems.
- Technology can be dehumanizing and thereby involves a loss of accountability. Examples include 1) the lack of naming in embedded systems and subsequent loss of authorization and 2) the lack of faith that a specific user has initiated a transaction vs. a specific device on his behalf (which may or may not have integrity). We need to be careful not to take the humans out of the loop too soon.
- The cost and inherent difficulties with device and strong user authentication result in choices that are more convenient and less costly to deploy – often resulting in user inconvenience, weak authentication, and subsequent weak authorization.
- Internet shortcomings are being transparently solved by overlay networks – examples include Voice over IP, SSL, and ANX – there is no single view of the network to manage and secure.

Privacy concerns abound. There is a drive to make customer relationships more intimate – a very positive thing. However, there are the opposing forces of user convenience vs. the need for privacy. There are unclear laws, regulations, or even generally accepted principles for organizations and individuals to set expectations by. Public availability of data mining tools makes highly sophisticated analysis and correlation available to many, and can result in unforeseen disclosure of information. If we do not adequately address the issues, loss of individual privacy will continue to increase and corporations will be frustrated by a game in which they do not know the rules.

Public policy is not keeping up with technology. Laws and regulations are often ineffective, inconsistent between countries, and do not address critical issues adequately (such as privacy and recent challenges with encryption). We are challenged by a world economy fractured by numerous individual government interests. Intellectual property laws and processes are not keeping up with "Internet speed." Monitoring, investigations, and prosecution are also difficult in this global environment. Yet, problems would be worse with involvement from government that is too heavy. Some fear that an existing "installed base" and information structure could begin to be a substitute for law. There is also a risk of security achieved in the future at a loss of individual freedom.

Copyright © 2001 Accenture. This document may, however, be reproduced and distributed.

Quotes from Deepest Concerns Discussion

These quotes capture part of the actual conversation during the discussion about concerns.

Law enforcement's ability to react, "*So my concern is in the electronic world, law enforcement is outgunned. I'm concerned about the Philippine-type attack where you know whether they actually physically originate here or not, bounce around enough places, cross enough borders, you don't have the laws in place to help you track them. The technology, in fact, makes it very difficult to map into the real world and get the human. Electronically we only have one-third of the protection. We might have electronic intrusion detection, but we don't have the equivalent of a local alarm and we don't have the law enforcement that's going to roll up within two and a half minutes if you live in the right neighborhood and actually arrest the guy once the alarm goes off."*

Getting the genie back in the bottle, "*We can't protect it now. I think we have to come back to terms with that. The fact is, because of the introduction of mobile agents, active desktops and other things, the genie and the bottle do not live in the same state*."

People are the problem, "*On the one hand, keeping honest people honest is a high goal everywhere. On the other hand, on the Internet, every sociopath is your next door neighbor."*

Copyright © 2001 Accenture. This document may, however, be reproduced and distributed.

The Call to Action

The future business models that rely so heavily on creating and forming temporary trust relationships in an interconnected, always-on world, drive us to work cooperatively to address these issues. The "We" in this call to action refers to members of business, consumer, government and academic communities working cooperatively to ensure a more secure future. In one participant's words, "*If we can increase the awareness we can help get closer to what is good enough and get active cooperation instead of active resistance.*"

Each of these areas in the Call to Action needs special focus and attention. We need to find champions and advocates for each of these areas. We need to look at what is being done in this area today, who are the players, where are the initiatives. We need to set specific objectives. Where do we need to be? What are the gaps? What is missing? What are the issues that need to be resolved? And we need to develop specific plans to achieve our objectives. As another participant stated, "*I think we've go to be careful not to let the perfect get in the way of the good. The solutions have to be realistic.*"

We need to work together to build assurances that the behavior we expect is the behavior we will get. We need to do this with an understanding that the electronic world is not a clean translation from the real world. Speed, connectivity, transparency, and complexity are compounding issues that impact our ability to solve these problems. Getting it right requires the greater community of business leaders, technologists, educators and political leaders to look seriously at each of these areas and commit resources and energy to lead us all to a more secure world.

Improve Software Quality

We need to focus some genuine efforts into improving the quality and assurance of software. We are building our future on a very shaky foundation. Weak and immature software is released and installed on operating systems with design and configuration security vulnerabilities creating a minefield of exposures. There need to be better inducements to design high quality software, to thoroughly test software products, and to provide quality assurance when delivering software on the Internet.

We need to do research in this area, to find better methods for designing and developing higher quality software. We need to develop new languages that do not allow buffer overflows and pointer problems and argument mis-matches, but have the potential for some re-use of libraries. This would solve a large number of the problems that occur today. In addition, a formal methodology for security testing needs to be developed and used.

We need to address accountability and responsibility in software design. We can no longer disassociate design and creation of software with losses and accidents that occur because of its use. Successful class action suits may provide some inducement to improve quality. Legal, political, regulatory and social systems may eventually add pressure. These systems, though, will never keep pace with the rate of change of technology. We must replace this weak foundation with something that can support the advent of such future applications as synthetic reality, virtual presence, autonomous agents, robots, open source and nanotechnology.

Copyright © 2001 Accenture. This document may, however, be reproduced and distributed.

Invest in Training and Awareness

We need a sound educational program that focuses on security and ethics. We must address the shortage of personnel with sufficient expertise. This should be done by focusing resources throughout the educational spectrum in K-12, University, and continuing education. People need to learn to respect electronic boundaries the same as we respect physical boundaries. They must understand at a very young age what is appropriate behavior, what is rude behavior and what is illegal behavior. People need to understand and question practices that compromise personal security and autonomy.

We need to define and teach baseline security lessons for different areas of study. Developers need much more training in designing developing secure code and secure systems. MBA's need to understand how to evaluate security risk in the context of the business environment. They need to understand their role in providing due diligence. Criminal justice students need to develop skills to deal with the electronic crimes. We need a whole new area of study to develop security specialists to fill the critical need today. We need a multi-disciplinary approach to training security specialists. There need to be joint efforts to develop a comprehensive curriculum to educate the next generation to deal with the complexities of all these trends identified at this roundtable.

Implement Best Practices

Incorporate baseline safeguards and practices, and develop metrics to gauge their usefulness. Best practices will provide guidelines for all of us to operate in ways that prevent unnecessary exposures. These need to be made available to everyone, not only to those who can afford it the most. We need to more effectively agree upon and adopt simple baseline security standards. Best practices are needed ,not only for producers of systems and software, but also for users. We need to be more convincing when we make the argument that standard components and standard methods free you to create the value you really should.

We need best practices for human resource departments when they evaluate candidates for jobs requiring the highest level of trust. We need best practices to protect firms as they connect electronically when they create temporary and permanent relationships with vendors, partners, customers. We need best practices for business managers as they evaluate risk in an environment where an unattended weakness can impact the reputation of the entire organization. We need best practices for consumers as they connect their personal devices to everything and everyone.

Many of these practices exist and are in use today, but it is not disseminated at a great enough depth to make a difference. People do learn and do adjust their behavior. We could start with a simple set of consumer practices and develop an international campaign to deliver the message.

Copyright © 2001 Accenture. This document may, however, be reproduced and distributed.

Initiate Public Debate
Initiate public debate to resolve the many issues involving ownership protection and use of personal information. We need to define what, where and when to protect information. We need to sort out all the tradeoffs we are making between convenience and privacy.

We need to reconcile the issues of information ownership, copyright and creative control. This is not simply a technology decision but a societal decision about how we are going to live our lives.

Advocate Holistic Approach
Advocate and pursue a well-rounded and pro-active approach to the overall problems: business, social, technical, and government. Few of the problems can be solved solely by a technology, a law, change in customs or business practices. We need to recognize the complexity of the problem and the relationships between people, process and technology. Policy is about the "thinking ahead of time" that companies need to do and about the exploration of unintended consequences. Policy issues will increasingly cross organizational and border boundaries. Policy and process issues include the legal system, customer expectations and privacy issues. People issues require identification and communication of expected behavior and enforcement of policies and processes to achieve that behavior. Technology implements policy and processes and relies on people to design, install, configure, and maintain the technology to achieve the desired behavior. These areas are inter-dependent, and therefore any security solution must address all of these areas.

Package Basic Security Architectures
Encourage packaging of a basic security architecture that provides standard services and integration with applications and infrastructure. PKI needs to be further developed and deployed where it can be useful and is appropriate. We need to address issues of key management, revocation standards, speed, and operation with varying certificate authorities. We need some reliable PKI structures with believable sponsors to enable many different things. We should consider the benefits of both certified and uncertified public keys. Simple stuff should be able to work without certification and yet it needs to be compatible. This is the issue of simple PKI and lightweight authorization vs. full PKI. We need to look at creating the ability to keep your signing capability (private key) on your person all the time, possibly in the personal assistant and eventually migrating to a token of the future.

We also need to invest real money in education and research to explore and discover security issues and solutions that will help us build a more secure world.

Copyright © 2001 Accenture. This document may, however, be reproduced and distributed.

Top Ten Trends - Detail

The following section provides more detailed background and context for each of the top ten trends.

The EverNet

Billions of devices proliferate that are always on and always connected.
Technology, culture and the law are all driving us towards this EverNet with millions and possibly billions of nodes always connected and always on. We are now seeing the explosion of attached nodes through the Internet and personal computing. Look for the super explosion to take off in cellular telemetry, particularly outside the U.S. Start thinking about every single object having an ID and being able to communicate, albeit in very short ranges. These nodes will not be only business to consumer, business to business, but business to device, consumer to device, and device to device. This always on, always connected environment also means that information exists in many places, in synchronized copy form, or flowing from to other points. In other words, information exists everywhere.

Technology is providing cheaper electronic transactions along with more single use and smart devices. At the same time society wants to use these technologies for instant gratification, such as web-enabled devices to check our stock prices in the elevator, monitor our teen driver's location and speed, or measure food and water to our dog's food dish. We want novelty, entertainment and cost reduction. We'll buy a clever device so that we can send e-mail between rooms in my home. We'll install a device in our refrigerator that will tell us when we need to order more milk and then order it. Our cell phones and PDA's will be enabled to conduct financial transactions from anywhere, and some of us will leave them on the bus or the airplane. What happens when these devices are disposable? How do you secure those transactions?

Businesses want to customize and maintain a continuous connection with their customers, to provide the right information, to the right person, at the right time, anywhere, to any device. Businesses also want to achieve economy of scale by moving things electronically. Legislation and a government desire to focus on the customer and reduce taxes is moving people on-line to pay taxes, register businesses, and apply for social services. In addition, we are finding that we need all these devices for survival. When our flight is cancelled, we need to instantly contact our travel service and grab a seat on the next flight out while all those unconnected people are still waiting in line.

This explosion of new networked devices increases the complexity of our systems to the point where it is not possible to comprehend all of what we are using. The interconnectedness of our systems is becoming so complex we will start to see emergent effects. The complexity itself will cause things to happen, power outages, network downtime, market crashes, enabling break-ins, that will catch us unprepared and incapable of identifying the causing factors.

The issues of identity and authority become highly visible as the number of devices explodes. How do you name all these devices? How do you bind the devices to an authorized individual or entity? How do you manage authorization decisions that limit the scope of activities allowed? People will delegate their autonomy to these devices which will make decisions on their behalf. We need authorization schemes that render lost and stolen devices unusable. Several devices can now represent an individual,

Copyright © 2001 Accenture. This document may, however, be reproduced and distributed.

creating identity conflict. We need authorization schemes that can deal with two devices making a similar request at the same time. The always on aspect means that millions of devices are now doing things, ordering products, updating software, changing data, when no one (or thing) is around to notice. Personal spying, too, becomes much easier when mobile devices deliver your geographical location.

This trend of billions of devices challenges security to become an enabler for assigning and validating identity. Passwords and the current web naming scheme will fail from sheer need for such a high quantity of devices. We are already past the stage where passwords provide meaningful protection. We must get better at delivering quality software that will not fail in economic high-stakes or life-threatening situations. There must be some process for assuring the safety and trustworthiness of software, similar to the trust we place in the electrical and natural gas industry. We need to reduce the need for continuous version updates or security hole fixes on billions of devices. Society needs to better understand how this proliferation could compromise their privacy and lead to loss of protection.

Copyright © 2001 Accenture. This document may, however, be reproduced and distributed.

Virtual Business

Complex outsourcing relationships extend trust boundaries beyond recognition.
Becoming an eBusiness is now necessary for survival. In one participant's words, "It's eBiz or bDead." The scarcity of specialized resources, the complexity of the infrastructure, the desire to transfer liability, and the competitive need to focus on core competency is driving many businesses to look for advantageous outsourcing relationships as they move into eCommerce. In addition, new relationships are being created by businesses that integrate, combine and resell services of multiple players in an industry.

This move towards outsourcing will create a huge increase in the number and complexity of business relationships that are created. Without proper precautions, there will be a noticeable lack of visibility and control around the outsourced business functions. This outsourcing trend will make it difficult for an industry to enforce its own business security policy on a process handled by multiple players.

Business processes could be subject to third party failures, in some cases, without even knowing about the dependency. This transition of trust will create a very complex value chain. For example, you have decided to host your eCommerce site on a service that offers "turnkey" business services. You sign a contract that specifies the size and power of the system you need, the amount of network bandwidth you require, the different applications you require to do business (including your accounting software, your human resource management software, database management software, shopping cart software, network management software, etc.), the type of web site you need for your business, and the management reports you want regarding the operation of your site. Although your contract is with this firm who may provide physical space, power, cooling, physical security, and network connectivity, the firm may have partnership arrangements with a wide array of vendors to which it subcontracts your tasks.

So, there may be separate firms handling each service feature and option for you, all transparent to you. However, as each of them may require access to your information and business resources, you have implicit relationships with all of them, though none are explicitly known to you. It will be difficult to know whom you trust, because you do not understand all the relationships and dependency that have been built around your business function.

The outsourcing companies themselves will need protection to prevent being targets of attacks (because they concentrate the data/functions for many clients), and to keep from being named as culprits if losses occur in other places.

When the security issues are properly addressed, this business model can lead to increased cooperation, contracts, monitoring and end-to-end control requirements. Awareness and knowledge of these issues and the security parameters will be critical for those developing these relationship models and crafting specific agreements. Technology tools for secure remote configuration and management and monitoring will be absolutely necessary. New processes and laws will be required to deal with those who will fail in these complex business arrangements. Individuals and small businesses who want to participate in this model with an even footing will need the services of a trusted third party to help them identify and negotiate with all the players.

Copyright © 2001 Accenture. This document may, however, be reproduced and distributed.

Rules of the Game

Government regulation increases as lawmakers react to real losses that hurt.
Government's role is to establish laws that ensure fairness, achieve public policy goals and balance conflicting societal goals. The EverNet is connecting ideologies, philosophies, economies and goals which have never before been connected or only tenuously connected. We must find a way to connect a world with different underlying motives and goals fairly, equitably, orderly and with minimal conflict. We must balance large scale economic interests with the rights of individuals. These conflicts will result in challenges to local rules, changes in law enforcement, and an emphasis on contract law as a means of settling legal disputes when they occur.

We will see increasing levels of crime that result in real losses that hurt innocent consumers. Governments will react as pressure mounts to do something to protect citizens. Money losses and economic affects, plus concern for damage to critical infrastructure information, will drive lawmakers to act. Information Warfare competition will be a smaller driver unless international events occur that raise the importance of military conflict. The focus of enforcement mechanisms, resolving legal disputes and dealing with network intrusions, will change from criminal to civil venues.

Governments' motivation to address network security threats increases as they enter cyberspace to conduct their business; collecting taxes, maintaining records, and conducting information warfare. Governments are also growing their capability to monitor communications. Centralization makes fixed information assets easier to police. When businesses are connected to automatically pay taxes, additional connections and operations are also possible.

The implications of increases in government regulation, especially if lawmakers feel compelled to "just do something", could produce unintended consequences that could be worse than the problems lawmakers seek to solve. The complexity of the issues, and the lack of awareness and understanding of technology within governing bodies makes this a likely scenario.

A particularly troubling scenario is the following: when lawmakers do not have the resources to investigate and enforce laws against prohibited activities, they may favor outlawing aspects of the technology itself. For instance, lawmakers might be tempted to outlaw the use of security technologies, because they have been known to be used by criminals. There is such a longstanding debate regarding vulnerability assessment tools. These tools are used both by attackers to identify likely targets, as well as security experts and managers, to determine what measures need to be taken to secure specific systems. Reactionary measures by lawmakers might attempt to curb open discussion of security flaws and vulnerabilities, which would handicap many private sector security managers and practitioners. Laws restricting system monitoring that are intended to protect privacy of users might be fashioned to be so restrictive that they preclude the use of intrusion detection systems and fraud detection monitoring systems.

Governments will find it difficult to determine the cost of defense against a network attack, because it is so difficult to determine the economic impact of attack. This, plus the need to protect critical infrastructure, is driving governments to work more cooperatively with industry. The United Kingdom, for example, has created a number of government/industry forums to address these issues. They have also announced plans to develop an electronics surveillance centre.

Copyright © 2001 Accenture. This document may, however, be reproduced and distributed.

Legal experts predict that, as the level of commercial activity increases on the Internet, the number of civil cases will rise commensurately. A significant number of those cases will deal with problems resulting from security or other incidents that occur because of faulty software or process. Expect to see class action suits against software vendors when major security events exploit software bugs causing economic hardship or failures. This may ultimately affect the way software is developed, tested and delivered. It could lead to third party software assurance services and massive growth in the Internet insurance industry.

This trend of government's increasing involvement will raise the issues of awareness regarding privacy, the need for software assurances, and software industry use of best practices. The public pressure upon government to act will drive changes in the law affecting the Internet that should be carefully analyzed for unintended consequences. Governments will recognize the need for more training in specialized security skills and may act to encourage skill building as national efforts. There will be increasing challenges and tension between federal and local law when crimes are international in scope, with no clear jurisdiction or sovereignty. Furthermore, as civil law is conducted by local governments, not federal, many large commercial disputes will be settled outside Federal government control This system will likely be tested with the globalization of commercial markets. For instance, we need to understand where to go to court for civil litigation in a globalized market.

Copyright © 2001 Accenture. This document may, however, be reproduced and distributed.

Wild Wild West

International criminals exploit lack of cooperation and compatibility in international laws. Crime in Cyberspace exposes the inadequacy of international laws and law enforcement. The I Luv You virus earlier this year, which caused significant economic damage to many companies, was released in the Philippines, a country with no laws on the book addressing these type of crimes. As companies become global, they will rely less and less on local governments who cannot help them when an international crime occurs on their networks and systems. "Everybody feels compelled to carry their own gun because "the law" is ineffective at stopping criminals." Large companies will become their own defensive force or they will do as businesses did in the Wild Wild West, they will hire private security companies to protect them in areas where the law is inadequate. In addition, international companies will use local laws to their advantage by picking the country whose laws they wish to apply to their business situation.

Consider the situation of a U.S. based global company that starts to recognize unusual behavior on their network. They trace the action across three borders to a country in the Middle East. Is this an issue of teen hacking, industrial espionage or electronic warfare? Is this the act of an individual, a crime syndicate, or a government conducting national espionage? How does this company engage multiple governments, who could be in conflict with each other, to track down crime? How does this company pursue legal remedy for a crime committed across boundaries?

Once again the security challenges call for implementing best practices to prevent and detect undesirable incidents, raising awareness and training among business managers and governments, using technology effectively to identify and track intruders, and working towards international laws that provide some ability to investigate and litigate international crimes.

Copyright © 2001 Accenture. This document may, however, be reproduced and distributed.

No More Secrets

Privacy concerns will continue to compete with convenience and desire for features
Privacy concerns are shaping a lot of what is being done and are driving decisions today. These concerns will drive even more decisions tomorrow as concern grows over what information is collected directly and what information is collected indirectly such as through cookies or data mining. At the same time most people seem willing to give up some of their privacy to accept a service that improves convenience or has nifty features. Will people continue to accept this situation or will there be a backlash?

Protecting customer privacy will also be a concern for businesses using customer information for competitive advantage. When I (as a businessperson) learn things about you and your needs that allow me to serve you better, that is context, the context of our relationship. Another businessperson who wants to compete with me will have to acquire what I already have, which is a context of your behavior. It's like when you go into the small town clothing store and somebody comes up to you and says, "Well Phil it's good to see you again. The things you like are over here." That is the context they have applied to serve you better. Context is what provides you with a sustainable competitive advantage and guarding that context is going to be quite important to holding onto your customers.

Another trend impacting privacy is the growing pressure for accountability. We need to know which individuals or organizations did things so that we can hold them accountable. This is not simply from the standpoint of a criminal or liability aspect, but simple business practice. We have to be able to determine who it is that we are dealing with in a business environment and to be able to assign some accountability for the actions that occur. That then is tied into the liability and insurance issue. At the same time, those who wish to protect their privacy will demand the ability to do business and yet maintain anonymity. Balance needs to be defined between personal privacy and the need to have identification for law enforcement and tax collection and national interest needs to investigate sedition, libel, etc.

Privacy can be said to have a low need for identifiability while accountability has a high-need to identify the individual or entity. As more value is placed into the infrastructure and the transactions, we have to be concerned with threats to that value and how we are going to go about recovering value in the event of loss.

The security challenges will be creating a secure infrastructure that can both provide accountability and protect privacy at a level that is acceptable to society. Accountability requires an ability to identify individuals and to have reasonable assurance that the device or system initiating the transaction truly does represent the identified user. This will become a huge issue as we transfer more authority to devices that can make transactions on our behalf when we are not present and not involved.

People need to have greater understanding of the tradeoffs they are making between privacy and convenience and businesses need to have a greater understanding of the liability they may incur if the information they are collecting and storing is misused. Public education and awareness, plus true public policy debates, are required to delve into the two sides of this issue.

Copyright © 2001 Accenture. This document may, however, be reproduced and distributed.

Haste Makes Waste

"Time to Market" increases pressure to sacrifice security and quality of software
The pressures to deliver at eSpeed to the market forces vendors to sacrifice security and quality for functionality and expediency. Weak and buggy software is delivered, and the buyers assume unknown risk when they deploy unsecured software. These problems are compounded when almost everyone uses the same standard software tools. The benefits of standardization, cost efficiencies and simplified interactions, become liabilities when weaknesses are discovered and exploited en masse in these products.

The classic theft of a credit card database from a web site in 2000 was successful because the web server software still contained a vulnerability that had been announced and the patch posted 18 months earlier. The February, 2000, denial of service attacks were successful because the attacker was able to load attack agents on thousands of systems containing identical known weaknesses that could be exploited by an automated tool. Today the easy path of compatibility is causing a lot of our problems. Developers are using old libraries, old programs, old operating systems, old programming languages. Because everything has got to be backwards-compatible, these problems are not being fixed as we move along. We are continuing to propagate and build upon bad solutions and known weaknesses.

The cycle of discovery and correction is failing in too many places. Weak, untested software is delivered and deployed in unsecured operating systems. Vulnerabilities are discovered and solutions (patches) are developed. Sometimes discovery is made by vendors and researchers. Sometimes discovery is made and acted upon. Sometimes solutions gets developed before exploitation is observed. Sometimes not. Sometimes the solutions are applied. Most times they are not. Some of the more enlightened eCommerce projects will include a quick vulnerability assessment as the last step before going "live". Even in these cases, there was probably no security expert involved in helping to build the initial architecture, and only rarely will a project build in time to the schedule for fixing any detected security problems.

Those with malicious intent create automated scripts to exploit these vulnerabilities and post the exploitation tool on the Internet. The exploitation script is designed to ferret out the systems that have not "patched" the hole. Now the expert has this incredible communication vehicle for transferring the ability to unskilled but motivated individuals. The skill-to-motive balance that existed in the past to prevent widespread attacks is diminishing. Attacks are becoming "shrink-wrapped". And those that have deployed but not patched the software are easy marks. The growing problem is the volume of easy marks.

You can read about intrusions and break-ins every single day in the press. Analysis of these events almost always shows that the attacker exploited a commonly-known and easily fixed hole.

Too many companies are not participating in this cycle of discovery and correction. In addition, the window is decreasing between the time when the vulnerabilities are discovered and when the mass exploitation begins. Patching vulnerabilities after discovery is not efficient and it is not safe. We need to deliver software with a higher level of assurance, rather than building elaborate mechanisms and processes to deploy corrections.

Copyright © 2001 Accenture. This document may, however, be reproduced and distributed.

Security will continue to be challenged by this capability. It has been observed that 20% of the traffic on the Internet is trolling, processes deliberately kicked off to look for weaknesses in network and system protocols. This translates to a high probability that our weaknesses will be probed and discovered. What happens when a group decides to launch a bunch of scripts at the same time with actual malice in mind? What will stop it? What will stop the copycats from doing it the next day?

When we build software that does not have basic protection features built in and say, "it's the user's responsibility to install anti-virus software because we have unconstrained macro usage in our program," that is not appropriate professional responsibility. Industry as a whole in this realm has been saying, "It's not my problem, it's pure technology – I'm just creating the technology, it's the user's problem." We cannot continue to do that. We actually have to start sharing the responsibility as developers. Producing nifty technology is great, but we also have to start thinking about how can that technology fit into the overall context – the Zen approach, where are the good parts, the bad parts, and what can we do in introducing that technology to make it worthwhile.

We need better software. We also need to develop some societal etiquette that addresses this type of rude behavior. We cannot wait until someone arrives at their first job and is told for the first time, "Thou shalt not do bad things with your computer." Education and expectations need to begin when children start using computers.

Copyright © 2001 Accenture. This document may, however, be reproduced and distributed.

Talent Wars

Lack of security skills will compound weaknesses of delivered solutions
People with deep security skills are very rare. Yet the demand for them is very high. We need these skills not only for designers, developers, and implementers of security solutions, but also for educators, managers, investigators, and others in critical roles which require a breadth of skill. The push for eCommerce requires a huge breadth of security skills to ensure accountability so that payments can be collected, to develop robust security architectures, and to protect personal and corporate assets.

The eCommerce application relies on an infrastructure that can tie one-time customers all the way back to corporate information deep in the data center. The complexity of the environment requires someone who understands about all the interactions of people, process, legal, and technology. This person must apply that knowledge to ensure the architecture, the infrastructure, and the development environment all work together to provide adequate protections for business and their customers. It will take a significant investment in time and money to define and build this rich set of skills that will be necessary for the future.

The public does not understand that the skill to break is not the same as the skill to build better. They would not hire a housebreaker to secure their homes, but they will hire people with a narrow focus on exploiting software vulnerabilities and a history of unethical behavior to tell them how to design robust solutions that involve policy, procedures, organization, infrastructure, and technology. Contrary to popular opinion, knowing how to exploit obscure holes in particular pieces of software is not a major prerequisite for the kinds of security specialists we need to help build a more secure world. Security designers must be well-qualified in the analysis and design of complicated inter-connected systems and we must be able to trust them to perform their design work in an ethical and professional manner.

Application developers are not trained in security and yet, some still design custom security solutions when a more robust and cost-efficient commercial product is available. Custom designed security solutions, engineered and developed by those untrained in security are rife with exposures. We need to remember that accidents as well as malicious intent can uncover these exposures and create damaging consequences.

All the elements of this expertise are not well-defined. They involve many different disciplines, computer science, psychology, law, mathematics, organizational design, etc. The traditional university approach does not deal well with this inter-disciplinary approach. There are very few universities issuing degrees in this area and even fewer that involve multiple disciplines**.** People are learning on-the-job and through several international training programs or security seminars. The areas covered by security are so vast, it is difficult to ensure that those learning security are grasping the complexity of the issue. There are some certification programs for specific technologies or security processes, but we should not place our confidence that this piecemeal approach will serve us well in the future. We must formally define the skills required for a security architect and other security specialties. We need to define a reasonable curriculum for each specialty.

Historically, we have built future skills in long-term research projects funded by government and leading edge technology companies (AT&T Bell Labs, government sponsored Arpanet). Where are the long-term investments in security research? Without these, we will have an incredibly difficult time

Copyright © 2001 Accenture. This document may, however, be reproduced and distributed.

developing solutions for the future. The drive for short-term solutions and the "first-to-market" is stifling our ability to invest in the future by funding research and education. The skills crises puts pressure on industry to hire people as quickly as possible instead of encouraging students and universities to build up a cadre to teach the next generation.

We need best practices to show people how to do security and we need trained professionals to teach people how to think security. We need to think about long term investments in training, education and research so that we can investigate and develop robust solutions for the future.

Copyright © 2001 Accenture. This document may, however, be reproduced and distributed.

Yours, Mine or Ours

Identifying intellectual property and information ownership will become key areas of debate
The explosive growth of electronic-based intellectual property and the easy ability to transform, manipulate and deliver the information anywhere, anytime, will force society into heated debates on ownership and control. In the world of paper, we understand that copyright means we can not reproduce text without someone else's permission. Yet, the common practice to forward emails and not even consider the duty to obtain consent is at odds with the current intellectual property law.

Authors have two different goals in protecting their intellectual property. They want to maintain creative control and they desire reasonable recompense for the energy, talent and training that is behind the words, ideas and formulas. The tension is growing in this area of recompense. Businesses are rushing to patent intellectual ideas for profit that others feel should belong in the public domain for the public good. As the employees with rare skills move from employer to employer, companies claim patents to protect their investments and maintain their advantage. Employees are given notice that these intellectual creations are not to be transferred to the new employer. This debate may lead us to creating new models for defining and compensating new intellectual property.

Creative control means that authors do not want someone to take their words or graphical design to endorse an activity irregardless of their intentions. They do not want anyone to morph their original composition into something over which they have no control. We can use watermarks and hash marks to maintain artistic control of documents we create.

There will be additional questions about what type of information we own and how we can control that. Who owns the information about my web habits, my on-line purchases? Who has the right to control that information? Who owns my medical records? The issues of ownership and control in these cases also relate to privacy.

The security challenges will be defining what where and when we need to protect information. Some information may only have value at a certain point in time, after that who cares? How do we know when that time has ended? What about when we successfully protect the transmission of information, via encryption, but do not protect the human interface viewing the clear text? The issue becomes one of ethics, when businesses are outsourcing the management of information they give people big windows into the business who may be bribed, or threatened into delivering that information into the wrong hands.

Copyright © 2001 Accenture. This document may, however, be reproduced and distributed.

Web of Trust

Standard security architectures and improved trust will spur eCommerce growth
Dynamic networks will continually appear and disappear to support temporary coalitions in business, government and the military. The dynamic nature of these networks, connecting mobile and wireless devices as well as remote networks, bring the issue of trust into the spotlight. How do you connect into the new environment and not disclose what you should not? What gives the local environment confidence in your identity? How do they know your system will not corrupt their environment? Both sides must have confidence that the interfaces conform to standards and neither end will pollute the other.

The basic issue is who do you trust and why? The *who* will be decided by the current situation and business opportunity. The *why* will be based on the security technologies that provide the ability to assure trust. Trust is not necessarily only on or off. There can be levels of trust, from low to very high.

The future will provide improved technology to enhance trust, including trusted third parties, industry-sponsored accreditation, digital identities, biometrics and smart cards. Standard security architectures will be developed that provide a set of security services like authorization, certificate management, encryption, and intrusion detection. These security services can be purchased from different vendors and integrated with various applications and the infrastructure.

Public Key Infrastructure (PKI) today provides components for a basic security architecture. It provides standard services that integrate with applications and infrastructure. These services include certificate management, directory services, encryption, integration tools, key management. A security technology like PKI has the potential to provide the benefits of standardization because, as it becomes more accepted, it becomes more economical. The viewpoint regarding one global public key infrastructure has changed over time. While there is no universal infrastructure that would enable any one person to use it in all circumstances, there are many global infrastructures that enable people to establish trusted relationships in a particular industry or environment.

These future technologies will face several challenges. As we continue to remove the human from transactions we will have reasonable confidence that a digital signature is difficult to replicate, but we may not have as much confidence that the object that was signed was actually viewed by any of the parties that signed it. Key management will continue to provide challenges, especially when multiple devices represent the identity of one individual. What happens when the key is stolen? How do you know? PKI may be useful and appropriate in many cases, but not necessary all. Issues still to be resolved involve revocation standards, speed, and operation and integration with varying certificate authorities. As more and more of the EverNet becomes PKI enabled and these issues are addressed, we will see more and more benefits in this architecture. We will also need to understand how to express and merge security policy in the technologies.

An explosion of much more powerful computers will impact our ability to implement stronger encryption and improve our level of trust. These powerful computers will also make it easier to break existing encryption methods. Those who lag behind in upgrading their security infrastructure will see their level of confidence diminish as their risk grows.

Copyright © 2001 Accenture. This document may, however, be reproduced and distributed.

Information Pollution

Information exploitation becomes more lucrative than hacking
People can exploit the speed and replicative nature of the net to manipulate markets and society for economic or political gain. The interconnectedness of everyone and our ability to spread and respond instantaneously to events, knowingly or unknowingly, increases the chance for misinterpretation causing havoc. Information pollution spreads when large databases contain unchecked, inconsistent and often incorrect data that is shared, processed, and used without careful monitoring.

There is an increasing trend towards information pollution where people are making more money by exploiting the connected society to manipulate people's perception of information than they are making by hacking anything. Consider Internet chat room postings to manipulate stock price. Society takes information from the marketplace. We manipulate it, we interpret, we analyze it, we push it back to the marketplace. Any one step missing or misinterpretation magnifies that all out of proportion. Something that came from one analyst in one little office with one small regional bank's interpretation of something suddenly becomes fact.

In a world where information is the coin of the realm, deliberately disseminated misinformation is forgery. The press recently reported the story of a teenage boy was charged in a "pump and dump" scheme. Having bought a few thousand dollars of penny stocks, he assumed multiple identities in various financial chat rooms, touted the stocks until the price rose, and then bailed out. What is surprising is not only the tender age of the perpetrator, but the apparent gullibility of the victims.

The gullible can also play a role in the transmission of misinformation. Countless virus hoaxes have transmitted themselves almost as quickly as actual viruses. One dire warning cautioned readers to be wary of magnetized tray tables on a certain airline, lest they erase one's hard drive.

People can also collect and interpret information about you to obtain competitive advantage. Consider intelligence gathering software agents that troll the net looking to see if what VPN client software you are running and to discover who else has this software. What are the communication paths? Now I can sell that information to someone who wants to discover with whom, how often, and when these communications occur. Does this mean a merger is on the horizon? Does this mean a product announcement will soon be released?

Mistakes are making their way into the global information ocean and we cannot remove them. The effort to obtain postcards for the dying boy does not die. The boy lives (cured in 1991), the world record has been set, and still this message is circulating and mutating. Even when it is not malicious, there is no way to ensure that information is accurate or timely. Search engines are polluted with false information, sending us to porn sites when we request information on a popular figure for our 7 year old child. As a society we are collecting and deciding based on inaccurate information.

Efforts need to be made to make sure information is timely and up-to-date. We need to know when information dies and can be buried.

Copyright © 2001 Accenture. This document may, however, be reproduced and distributed.

About Accenture

www.accenture.com

Accenture, formerly known as Andersen Consulting, is an $8.9 billion global management and technology consulting organization. The firm is reinventing itself to become the market-maker, architect and builder of the New Economy, bringing innovations to improve the way the world works and lives. More than 70,000 professionals in 48 countries deliver a wide range of specialized capabilities and solution to clients across all industries. Under its strategy, the firm is building a network of businesses to meet the full range of client needs -- consulting, technology, outsourcing, alliances and venture capital.

Accenture is recognized as a leader in information security. Our proven approach clarifies the issues and provides a clear roadmap for security planning. We focus on business strategy and security implementation, not just audits. We offer full service security solutions and in-depth technical expertise to solve the complex challenges of the evolving business environment.

About CERIAS

www.cerias.purdue.edu

The Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue University is the world's leading academic organization in its field. The Center's goal is to promote and enable world-class leadership in interdisciplinary approaches to information assurance and security research and education. This is accomplished through the financial and technical support of industry and government partners, and the active participation of researchers from across Purdue's many schools and departments. Over 100 faculty, staff and students at Purdue are currently involved in leading-edge efforts at improving the practice and knowledge of how to secure information systems in today's rapidly-changing environment.

Copyright © 2001 Accenture. This document may, however, be reproduced and distributed.