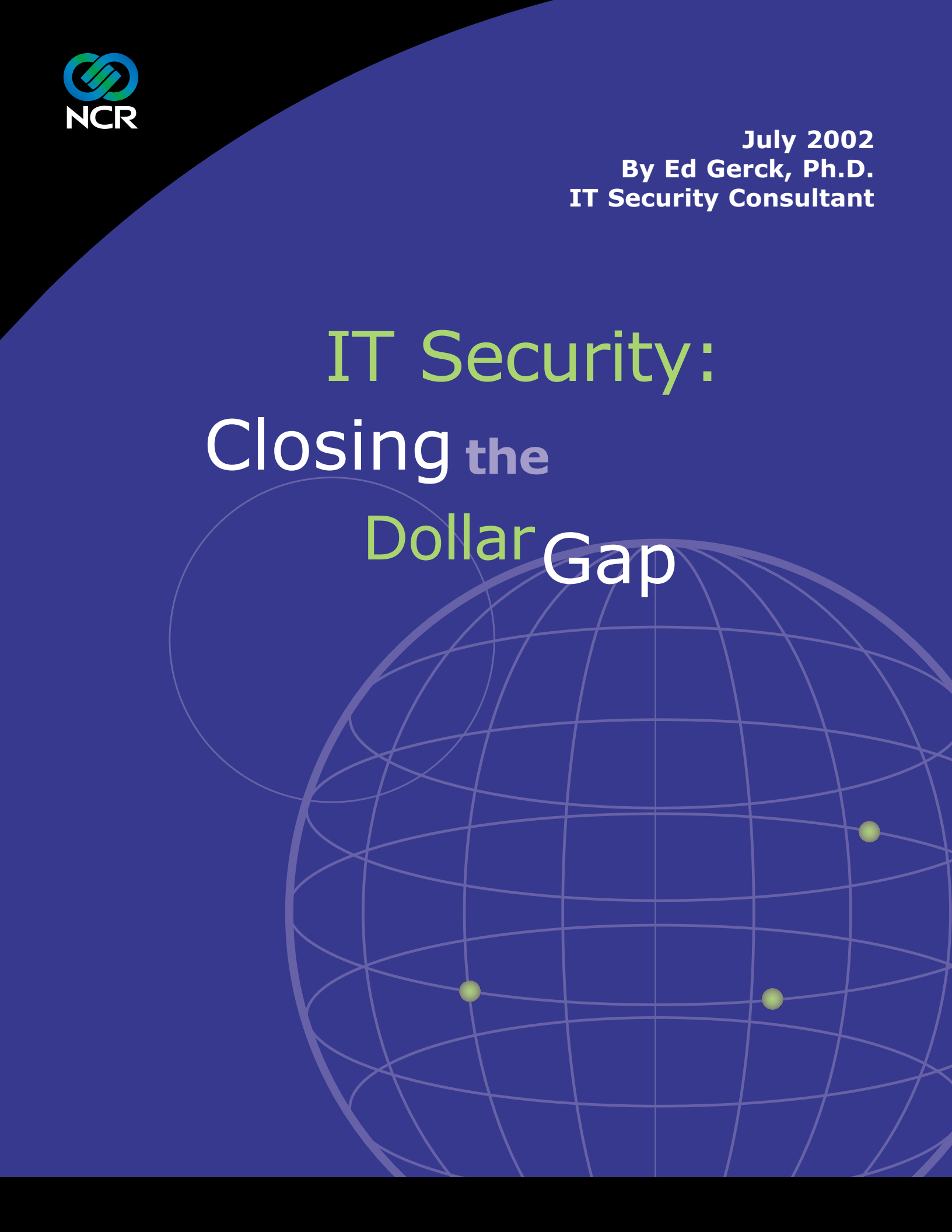


July 2002

By Ed Gerck, Ph.D.
IT Security Consultant

IT Security: Closing the Dollar Gap

Most security products profess to solve broad problems when enterprises really need **specific solutions.**

Executive Summary

It is unlikely that a commercially available IT security system completely meets enterprises' requirements – and if it does so today, it will not do so tomorrow. Hackers, crackers, bugs, insecure operating systems and business evolution will always be a fact of life and, as a result, new security threats and holes will constantly appear. All of today's security solutions will need to be continually updated to remain effective: they will need patches, upgrades, support and perhaps replacement to provide the same amount of value tomorrow.

In this scenario, IT security solutions usually have a large gap between the expected dollar benefit and the actual dollar benefit, which gap we call the "dollar gap." The dollar gap should ideally be zero. A smaller-than-expected dollar benefit means the security solution is not as effective as desired. A larger-than-expected dollar benefit means the security solution was not optimized in terms of company resources. **The larger the dollar gap, the less the dollar benefit that could have been obtained.**

To make matters more complicated, an enterprise usually does not have the highly specialized, expensive resources in house that would be needed in order to define, develop and validate an IT security solution that would meet those requirements.

Thus, enterprises usually rely on a security service provider that can help identify vulnerabilities and risks in target systems and environments, develop an enforceable security policy with clear and concise standards, provide proof-of-concept testing to validate the recommended security architecture, document and deploy the IT security solution, train personnel and support the solution.

NCR is a security service provider that exemplifies the needed IT security service capabilities, capacity and quality required to help clients address their IT security needs on a global basis for retail store automation, financial self service and payment and data warehousing.

The Ever-Present Threat

The business problem of information security is that security solutions require continuous, onerous cycles of development and maintenance.

Hackers, crackers, bugs, insecure operating systems and business evolution will always be a fact of life and, as a result, new security threats and holes will constantly appear. All of today's security solutions will need to be continually updated to remain effective: they will need patches, upgrades, support and perhaps replacement to provide the same amount of value tomorrow.

The dilemma facing enterprises is that while the cost of doing nothing is increasing, the needs seem to outpace the solutions at an ever-faster pace. Security challenges are increasing and change is a constant. According to CERT [1] data, the number of security incidents per year is increasing at a rate larger than the number of Internet hosts.

The Dollar Gap

The Dollar Gap

In a survey published in January 2002, Tech Update reported that IT managers are no longer focusing purchases on technology for technology's sake, but on strategic systems that bring an immediate dollar benefit to the business. Dollar benefit includes revenue, cost avoidance and cost savings.

However, estimating the immediate dollar benefit in IT security seems to be as difficult as predicting the weather. IT security solutions usually have a large gap between the expected dollar benefit and the actual dollar benefit, which gap we call the "dollar gap." The dollar gap should ideally be zero. A smaller-than-expected dollar benefit means the security solution is not as effective as desired. A larger-than-expected dollar benefit means the security solution was not optimized in terms of company resources. The larger the dollar gap, the less the dollar benefit that could have been obtained.

The usual large dollar gap in IT security solutions not only makes IT security more expensive than it would look at first sight, it also makes IT security less efficient by increasing the number and extent of security gaps. Security gaps represent the weak areas that could be attacked in an IT system.

In a broad generalization, two types of attacks can exploit security gaps: network and data attacks. A network attack tries to interfere with client and/or server systems that participate in a transaction in terms of their communication processes. A network attack, for example, may try to gain or deny access, read files or insert information or code that affects communication. On the other hand, a data attack tries to tamper with and/or read data in the files or messages as they are stored or

exchanged in a system, for example by inserting false data, by deleting or changing data or by reading the data.

Therefore, an effective IT security methodology must address not only the security gaps, but also the dollar gap.

How Can We Reduce the Dollar Gap?

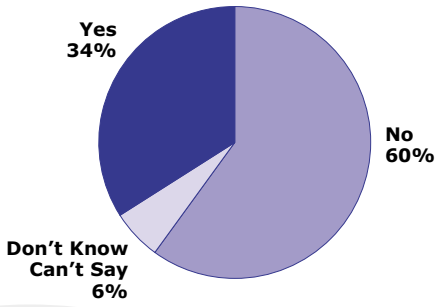
Experience shows that reducing the dollar gap in IT security calls for highly skilled security professionals, a thorough analysis of the system's requirements and risks, a unique blend of COTS ("commercial off the shelf") tools and proven methodologies to deliver and support the solutions. For example, given a system with a desired security policy for access control, a security policy must define an implementation of the policy that can enforce the security objectives when all operational factors are taken into account, providing for effectiveness assurances in addition to correctness assurances.

However, quantifying losses in order to define risk for a security policy is easier said than done. According to a 2002 survey by Forrester Research, most (60%) IT managers are unable to quantify their business loss resulting from security incidents. This means surveys on the cost distribution of security breaches, such as that provided by the U.K. Department of Trade and Industry, may not provide a reliable estimator of how much might be at stake in security breaches.

Fraud is insidious and law enforcement is too sluggish in moving against automated fraud and con games. That is why an IT security system also needs to keep every advantage, both from external as well as from internal attackers, so that attacks can be forestalled as much as possible and not cost time and resources in defending against them.

Quantifying Loss

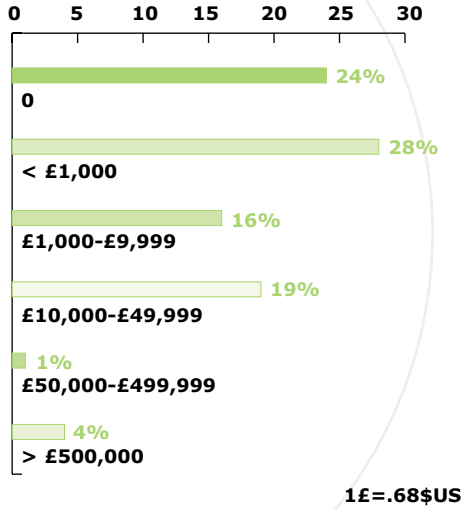
Are you able to quantify the business loss from security incidents?



Source: Forrester Research (www.forrester.com)

Cost of U.K. Breaches

What was the cost of your worst security incident in the last 12 months?



1£=.68$US

Source: U.K. Department of Trade and Industry (www.security-survey.gov.uk)

The Technical Problem of Information Security

An IT security system must avoid the scenario of a single point of control, which can be recognized as a single point of failure.

The technical problem of information security is to avoid too much concentration of information and power, while allowing enough information and power so as to make a task possible to execute. An all-knowing, all-powerful entity would be the perfect attacker and could break any security measure. That is why we oftentimes talk about "need to know" and "separation of powers." We name these principles, respectively, information granularity and power granularity. These principles mean that information should not be provided in its entirety to a single entity and one should also avoid the scenario where any entity is, at the same time, user, administrator and auditor. Business information and power should therefore be carefully divided, for example, among local employees, the office management, the enterprise management and the end-user. And, contrary to what is oftentimes still advocated, there should be no single point of control in an IT security system, which we would need to recognize as a single point of failure.

Tools such as authentication and authorization can help define information and power granularity. However, at its most basic level, a secure IT system needs to do much more than just control authentication and authorization. No matter how much assurance is provided that each component of a secure system is correct, when operational factors such as collusion, internal attacks, hackers, bugs, viruses, worms or errors are taken into account, the system may fail to be effective (i.e., may fail to be secure in the context of its operational use). In addition, underlying assurance problems such as insecure operating systems and reoccurring buffer overflow vulnerabilities are not likely to improve over the coming years.

There is a real need to bring together policy, management and implementation considerations that could influence effectiveness assurances for each particular IT security solution.

Consequently, there is a real need to bring together policy, management and implementation considerations that could influence effectiveness assurances for each particular IT security solution. Other security principles such as redundancy, diversity, no single point of failure and least privilege also need to be used in defining the specific requirements for a secure IT system. In addition to being specific, such requirements need to be clearly formulated, decidable and, as much as possible, complete [2]. Additionally, an end-to-end design is important to assure effectiveness [3].

For lack of paper trails, non-repudiation is also essential for Internet and IT security systems. A common definition states that non-repudiation is about providing proof that a particular act was actually performed, for example as demonstrated by a trusted time stamp. However, the concept of non-repudiation may also be taken in a much stronger sense in support of the business needs of a particular application, meaning to prevent the effective denial of an act [4].

Commonly, IT secure systems must also satisfy security standards such as the Controlled Access Protection (C2) level of security as defined in DoD 5200.28-STD

(the Department of Defense Trusted Computer System Evaluation Criteria), the ITSEC Level 3 as defined in the Common Criteria for Information Technology Security Evaluation or the Code of Practice for Information Security Management BS 7799 (a British Standard that is the basis of the ISO/IEC 17799-1 Standard).

To meet these objectives, an effective security engineering methodology should be based on two points:

- Clear security principles, algorithms and products based on time-proven designs; and
- An independent, permanent verification and validation of the system's security features.

The first point defines the component quality used in the IT system, where a weak component may compromise the whole system. The second point focuses on the need to continuously evaluate all potential and existing threats, and verify any additional security design features that might be necessary to mitigate the risks stemming from the most likely and/or most damaging threats associated with the customer environment, and eventual changes in that environment.

Effective IT Security Methodology

An effective IT security methodology must deal with an extensive list of security properties. It is the adequate combination and interoperation of security properties that provide the usually required resiliency of a secure IT system, which must not "pop" like a balloon when subjected to an attack, or fail silently leaving no trace of the attack. There must be multiple channels of communication and correction, even if the channels are not 100% independent [5].

The most important security property is trust [6]. Risk, for example, can only be defined after one defines what is at risk, and what is at risk must be that which is trusted to some extent, otherwise there would be no risk. In other words, risk has to do with the loss and probability of loss, but only the loss of what is trusted would affect the system.

IT security solutions need to bring together policy, management and implementation considerations that could influence effectiveness assurances for each particular solution.

In addition to trust, several security properties are frequently required in IT security systems, including:

The 10 Basic Security Properties

Access control	Gaining access to objects, based on the trusted identity of users; limiting access to system resources only to authorized users, processes or systems.
Audit	Maintenance of a historical log of all transactions that can be reviewed to maintain accountability for all security-relevant events.
Authentication	Corroboration of a credential or claim; the ability to establish and verify the validity of a user, user device or other entity, or the integrity of the information stored or transmitted.
Authorization	Conveyance of rights, power or privilege to see, do or be something.
Confidentiality	Ensuring that data is not available or disclosed to unauthorized individuals, entities or processes.
Integrity	Ensuring that data is not altered or destroyed in an unauthorized manner.
Non-repudiation	The ability to prove the origin and delivery of transactions; the ability to prevent the effective denial of an act.
Process validation	The ability to periodically validate the correct operation of the solution's processes and security functions.
Security management	A defined process to perform system security functions such as audit, PKI management and configuration management.
Trust	Qualified reliance on information; trust is that which is essential to a communication channel but cannot be transferred through that channel.

Additionally, specific security requirements and properties may:

- Ensure that system functionality and data are available as required to meet operational requirements.
- Identify and authenticate the identity of users prior to granting them the appropriate system access.

- Prevent the unauthorized disclosure or dissemination of data.
- Prevent unauthorized modification of system components.
- Provide mechanisms and procedures to detect system failure and prevent degradation of security processes.
- Provide each processing site with authorization for the information being processed.
- Be accessible only to individuals authorized for the information being processed at that site.
- Provide contingency plans that will be maintained for emergency situations and disaster recovery.
- Provide configuration management that shall be enforced to control all physical, hardware, software, firmware and documentation changes.
- Provide system administrators and users trained to operate the system in a secure fashion in accordance with a security policy.
- Record and provide tools for the analysis of significant security events.
- Make audit analysis available and controlled so as to be performed only by authorized system administrators.
- Maintain audit logs for the duration of system operation that are archived to conform to corporate, county, state, federal and international requirements regarding the preservation of records.

Provision of the 10 basic IT security properties, along with the additional properties listed above, also needs to rely on reasonably independent certification and accreditation procedures to assure their effectiveness. For example, producing the required evidence to support an informed decision as to whether to grant approval to operate the solution with an acceptable level of residual security risk or not to grant such approval.

Security Service Providers

It is unlikely that a commercially available IT security system completely meets the enterprises' requirements – and if it does so today, it will not do so tomorrow. To make matters more complicated, the enterprise usually does not have the highly specialized, expensive resources in house that would be needed in order to define, develop and validate an IT security solution that would meet those requirements as outlined in the previous sections.

…enterprises usually rely on a security service provider that can help identify vulnerabilities and risks in target systems and environments, develop an enforceable security policy with clear and concise standards, provide proof-of-concept testing to validate the recommended security architecture, document and deploy the IT security solution, train personnel and support the solution.

Considerations in Selecting Security Service Providers

Thus, enterprises usually rely on a security service provider that can help identify vulnerabilities and risks in target systems and environments, develop an enforceable security policy with clear and concise standards, provide proof-of-concept testing to validate the recommended security architecture, document and deploy the IT security solution, train personnel and support the solution.

A security service provider, in addition to any particular vendor's solutions, should investigate a broad range of solutions and technologies, using COTS products and systems to the greatest extent possible, modifying existing applications where appropriate and developing new components and interface capabilities where required, in order to provide full functionality with the least dollar gap.

In other words, a security service provider must not consider an IT security solution as just a firewall or even a collection of COTS products to be installed. Oftentimes interface code needs to be developed by the security service provider or by a third party in order to reduce modifications of the COTS products (to prevent losing track of COTS version changes) and to provide collective functionality. The solution's functional requirements may also motivate engineering modifications to be introduced by a vendor into their COTS product as an alternative, for example, to the increased complexity of using more COTS modules with higher cost and reduced end-to-end security. Code development versus adding new COTS products (the creator verses integrator views) versus requesting COTS modifications is a decision process that must answer a number of questions, including:

- Which technologies and products are most appropriate?
- How can product mismatches be rectified in our system?
- How can we engineer system attributes such as reliability, security and performance in spite of decreasing control over individual system components that come from COTS products and their changing versions?
- How do we integrate new COTS products with the custom code we already have?
- How do we take advantage of COTS while delivering a solution that can evolve over a long lifetime?

These points are central for reducing the dollar gap and creating conditions for a favorable ROI.

The Importance of a Solution Development Methodology

To provide full solution functionality with the least cost, the security service provider needs to apply a **solution development methodology** that simultaneously considers the solution's requirements, cost, schedule, operating and support environments, capabilities of products in the marketplace and viable architectures and designs. All these items are dynamic and interact with one another.

The first challenge of the solution development methodology is to adequately define the solution's requirements. Second, the solution development methodology should leverage the initial development effort into a finished product with the least rework. The third challenge of the methodology is the high level of assurances required to "do it right the first time." Here, experience and proven performance must outweigh potential gains. The solution development methodology should preserve the proven performance of any selected COTS product.

…challenges exist in any solution's development, the foremost being the risks associated with incorrect and optimistic status reporting.

Additional challenges exist in any solution's development, the foremost being the risks associated with incorrect and optimistic status reporting. One of the most common sources of problems in COTS-based software development is the fact that software project status reports are oftentimes not accurate even though they may seem to be believable. Far too often, monthly status reports are optimistic that all is on schedule and under control until shortly before the planned delivery, when it is suddenly revealed that everything was not under control and another six months may be needed. **But usually, a business solution's deployment has a deadline that is quite unmovable.** The solution's project status reporting needs to address this concern head on, including progress tracking and realistic metrics. Monthly status reports with earned value measures should be used as a tool to give the enterprise and the project managers a clear and precise indication of everything that is right and everything that is wrong with the condition of the project as of the current moment.

To reduce rework and missed expectations in the solution development, the security service provider should require testing or credible test references for all COTS components, including hardware, software design tools, compilation tools, debugger tools and any other tools that may be considered for use in the solution.

Additionally, the solution development methodology should include security professionals in that solution space, who should act as verifiers during the entire design phase and not just during validation and verification.

The various components of the solution need to be integrated. The solution development methodology should include integration testing to verify that system functionality conforms to requirements. Integration testing should be done in two phases – validation and verification. Validation involves consultations with local

users, corporate offices and legal bodies in order to confirm the operational assumptions of the solution. Verification involves actual system testing in order to confirm the validated operational assumptions are met in conditions as close as possible to the expected operating conditions. The enterprise should observe both phases. When everyone is satisfied that the system is ready, the configuration should be frozen and the system turned over to the enterprise for certification testing before it is actually used.

Finally, avoiding those issues and conditions that tend to lead to rework should be a main focus of the solution development methodology. Risk management measures need to be used, including schedule time for minor system rework to address any anomalies identified in testing.

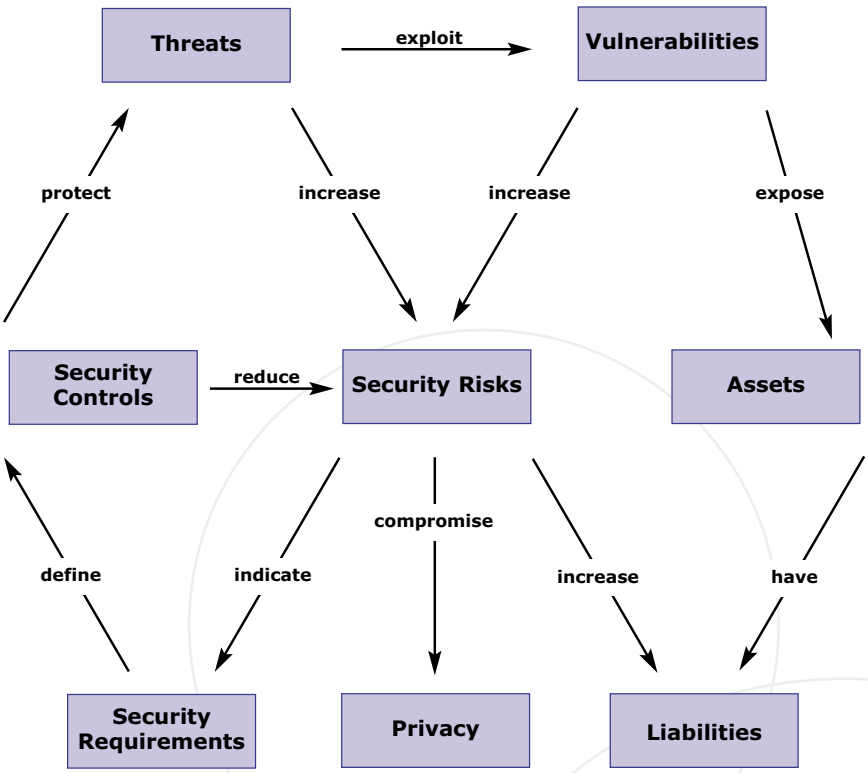
The NCR Example

NCR is a security service provider that exemplifies the needed IT security service capabilities, capacity and quality required to help clients address their IT security needs on a global basis for retail store automation, financial self service and payment and data warehousing.

NCR is present in over 120 countries and territories with over 30,000 employees worldwide. NCR offers a good example of an effective security methodology that has been successfully applied to a large number of IT security projects.

In implementing an effective security methodology, NCR uses certified COTS hardware and software including firewall, intrusion detection systems, web and e-mail content filtering, virtual private networks, securing remote access, wireless technologies and virus protection. NCR also follows the Code of Practice for Information Security Management BS 7799 (a British standard that is the basis of the ISO/IEC 17799-1 Standard) and other standards as may be required by the enterprise's solution (including X.509 and PKIX, for example). This approach is based on a comprehensive risk assessment and risk management matrix, which is graphically indicated on the following page.

The Risk Assessment & Management Matrix



NCR is an approved Cisco Security Services partner for vulnerability assessment, design and implementation, policy and procedure, and business impact and risk assessments. NCR is also an approved VISA security assessment provider. This designation allows NCR to perform security assessments for VISA merchants or service providers to ensure they comply with VISA program requirements.

NCR demonstrates the in-depth expertise and multi-vendor approval required to plan, develop, manage and maintain today's global IT security systems.

Notes

1. The CERT® Coordination Center is part of the Software Engineering Institute. The Software Engineering Institute is operated by Carnegie Mellon University for the Department of Defense. The website is www.cert.org.
2. Security requirements form a logical system of some complexity and thus we do not expect such a system to be both complete and consistent. See Goedel's incompleteness theorem.
3. Attacks and errors are hard to detect and prevent at the interface points.
4. To be effective, non-repudiation needs to take into account technical and business considerations. For example, bank checks are non-repudiable in the sense that a check is paid if (1) you did not tell the bank beforehand that the check should not be paid and (2) the signature does not look like a signature you did not make. The reader should note the double-negative, which provides less room for customer repudiation – the signature does not have to look like a signature that you made, it just has to not look like a forgery.
5. If two communication channels are not 100% independent (but not fully dependent), the probability that two channels may be compromised at the same time is smaller than that of any single channel.
6. In terms of a communication process, trust has nothing to do with feelings or emotions. As defined by Ed Gerck, trust is qualified reliance on information, based on factors independent of that information. In short, trust needs multiple, independent channels to be communicated. Trust cannot be induced by self-assertions. More precisely, "Trust is that which is essential to a communication channel, but cannot be transferred using that channel." See "Trust Points" by E. Gerck in "Digital Certificates: Applied Internet Security" by Jalal Feghhi, Jalil Feghhi and Peter Williams, Addison-Wesley, ISBN 0-20-130980-7, pages 194-195, 1998.

About the Author

Dr. Ed Gerck is a recognized leader in Internet security and cryptography, with six recent pending patents. He has a doctorate in physics from Ludwig-Maximilians-Universitaet and Max-Planck-Institut fuer Quantenoptik, in Munich, with maximum thesis grade. With a background in lasers and quantum mechanics, he has worked in cryptography since 1987. His work in Internet security, cryptography and safe Internet voting has been widely published and has also received extensive worldwide press coverage from the *New York Times, Le Monde, O Globo, Forbes,* CBS, CNN, *Business Week, Wired* and *USA Today.* Dr. Gerck can be reached by e-mail at egerck@nma.com.

WCS-1028 0702