The Software Quality Advisor Online

Rice Consulting Services, Inc.
P.O. Box 891284
Oklahoma City, OK 73189
405-793-7449
405-793-7454 FAX
November 2001

The Threat of Cyber-Terrorism

by Randy Rice, CQA, CSTE

With the recent terrorist attacks, many security experts are concerned about the threat to information assets in the United States. While information security has been a key concern since the proliferation of computer networks, the increased levels of concern has prompted us at RCS to devote more resources to help combat this threat.

As described in the November 5th issue of Information Week magazine, *"The effort to improve computer security is driven by two truths that aren't likely to change: Networks need to be open, and software is essentially imperfect--both of which mean hackers will find their way in."* The article goes on describe new ways that research is being conducted in securing systems besides the traditional firewall approach. The problem with firewalls is that there are holes and the crackers seem to have skills at finding and exploiting them. You can read the article at http://www.informationweek.com/story/IWK20011102S0012

One of the conclusions that IT security professionals and researchers have reached is that future attempts to realize effective security will require creative and fundamentally different approaches. We know that we can't rely on vendor solutions alone because to date the levels of quality don't meet the requirements of hack-proof software. At the same time, we know that people need access to certain systems. To make matters even more complicated is the impact of "human engineering" where intruders can fool humans into giving them access to otherwise secure systems.

Until that time when new and creative solutions are realized, interim measures will need to be applied diligently. As many security experts will testify, it's the loose security of others that cause problems for everyone else. Hopefully, it won't take a major cyberterrorism attack to bring a sense of urgency to this issue. In this spirit, I write this article and hope to give you both a background on the topic and ways to prevent attacks. In addition, I will also discuss strategies to help you test the adequacy of security solutions.

What is Cyberterrorism?

According to the U.S. Federal Bureau of Investigation, cyberterrorism is any "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents." [1]

"Unlike a nuisance virus or computer attack that results in denial of service, a cyberterrorist attack would lead to physical violence or extreme financial harm. According to the U.S. Commission of Critical Infrastructure Protection, possible cyberterrorism targets include the banking industry, military installations, power plants, air traffic control centers, and water systems." [2]

"Cyberterrorism is sometimes referred to as electronic terrorism or information war." [3]

As if the cyberterrorism threat is not enough, there is the related threat of organized cybercrime, which has been blamed in recent cases of e-commerce extortion and online fraud. As Phil Williams, Professor of International Security Studies at the University of Pittsburgh writes,

"Organized crime groups typically have a home base in weak states that provide safe havens from which they conduct their transnational operations. In effect, this provides an added degree of protection against law enforcement and allows them to operate with minimal risk. The inherently transnational nature of the Internet fits perfectly into this model of activity and the effort to maximize profits within an acceptable degree of risk. In the virtual world, there are no borders, a characteristic that makes it very attractive for criminal activity. When authorities attempt to police this virtual world, however, borders and national jurisdictions loom large -- making extensive investigation slow and tedious, at best, and impossible, at worst.

The Internet itself provides opportunities for various kinds of theft, whether from online banks or of intellectual property. But it also offers new means of committing old crimes such as fraud, and offers new vulnerabilities relating to communications and data that

[1] www.searchsecurity.com
[2] ibid
[3] ibid

provide attractive targets for extortion, a crime that has always been a staple of mafia organizations.”[4]

Williams’ conclusion is not very encouraging. “In sum, the synergy between organized crime and the Internet is not only very natural but also one that is likely to flourish and develop even further in the future. The Internet provides both channels and targets for crime and enables them to be exploited for considerable gain with a very low level of risk. For organized crime it is difficult to ask for more. It is critical, therefore, to identify some of the ways in which organized crime is already overlapping with cybercrime.”[5]

From professor Williams’ observations and predictions, the threat of cyber crime is one to be taken just as seriously as cyber terrorism. A major issue is getting people at the grass roots level in organizations to realize the credibility of the threats.

How Real is the Threat?

This threat is certainly a clear and present danger. Consider the following:

- This year, the Code Red virus infected over 760,000 computers worldwide and was the fastest spreading virus seen to date over the Internet.

- “Symantec's CTO Rob Clyde notes that there are now so many free tools on the Internet that hackers needn't be experts to cause problems; all they have to do is run readily available scripts. And with 97% of the world's money supply in digital form, hacking as an intellectual exercise will rapidly give way to cybercrime for profit, he predicts.”[6]

- “Following the United States' first strikes against sites in Afghanistan, Attorney General John Ashcroft said last week that the FBI and other federal law-enforcement officials had advised thousands of CIOs, chief technology officers, and IT managers that their IT systems may be targeted in retaliatory terrorist attacks-or used to launch them. As companies heed Ashcroft's advice to maintain "the highest state of alert," the way they do business may change.”[7]

- “In the aftermath of the 11 September attacks, hacking groups have formed and participated in pro-U.S. and anti-U.S. cyber activities, fought mainly through web defacements. There has been minimal activity in the form of DDoS attacks, mostly between opposing protesting groups. NIPC has reason to believe that the potential for future DDoS attacks is high. The protesters have indicated they are targeting web sites of the U.S. Department of Defense and organizations that support the critical infrastructure of the United States, but many businesses and other organizations—some completely unrelated to the events—have been victims.”[8]

“Preparedness for cyber terrorism, which we have described often in our discussions as a weapon of mass disruption, if you will. But make no mistake about it, this disruption can be a very deliberate attack on the capabilities of the United States to respond to any other type of attack, or even to end civilian life if in fact our processes through the Internet, and our other information technology capabilities are attacked deliberately.

Our preparedness for cyber terrorism must be broader, to include all levels of private and public activity. Critical local, state, regional and national systems are computer controlled -- computer controlled -- that is the world that we now live in. Power grids, communications, airlines, hazardous materials, hospital life support, the nation's economy, and our national defense.

For years terrorism has been viewed as the exclusive domain of national security. That view requires a reality check. The federal government must recognize that states, communities, governors, mayors, and citizens all have responsibilities, and important vital roles in dealing with the terrorist threat.”

Gov. James Gilmore

Chaiman, Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction

[4] Organized Crime and Cybercrime: Synergies, Trends, and Responses, Prof. Phil Williams, http://usinfo.state.gov/journals/itgic/0801/ijge/gj07.htm
[5] ibid
[6] Zeroing In, Information Week, November 5, 2001
[7] IT on High Alert, Information Week, October 15, 2001
[8] Advisory 01-026, National Infrastructure Protection Center – www.nipc.gov

How are we Doing?

Based on recent surveys and the information presented to congressional hearings, we have a long way to go before security threats are adequately addressed.

"According to InformationWeek Research's 2001 Global Information Security Survey, fielded by PricewaterhouseCoopers from April to July. Almost half of 2,131 U.S. companies surveyed had no formal security policies in place, and most relied primarily on user passwords and multiple logons for protection." [9]

"Only 49% of U.S. companies had plans to raise user awareness of policies and procedures in the next 12 months." [10]

"What's more, only half of 150 companies surveyed by InformationWeek Research one week after the terrorist attacks say they plan to reassess the security of their facilities in light of those events. "We need more people to be doing more creative thinking about computer security," U.S. Rep. Sherwood Boehlert, R-N.Y., said in a House of Representatives Science Committee hearing last week on the security of the nation's corporate IT infrastructure. "That's what our adversaries are doing." [11]

How Could the Threats Play Out?

In December, 2000 the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (a.k.a. The Gilmore Commission) released their second annual report which stated two possible cyber terrorist scenarios. First, "It is easy to envision a coordinated attack by terrorists, using a conventional or small-scale chemical device, with cyber attacks against law enforcement communications, emergency medical facilities, and other systems critical to a response." [12]

Second, "it is conceivable that terrorists could mount a cyber attack against power or water facilities or industrial plants -- for example, a commercial chemical plant that produces a highly toxic substance -- to produce casualties in the hundreds of thousands." [13]

The report adds that "the most likely perpetrators of cyber-attacks on critical infrastructures are terrorists and criminal groups rather than nation-states." [14]

Best Practices

So, what can be done proactively to prevent cyberterrorism and cyber crime attacks? One source of best practices for security can be found at the Computer Emergency Response Team's (CERT) web site at http://www.cert.org/security-improvement. This is a rich resource for anyone looking to implement or improve security practices. I highly recommend it!

CERT's five areas of practices are divided into:

1. Harden and secure your systems by establishing secure configurations
2. Prepare for intrusions by getting ready for detection and response
3. Detect intrusions quickly
4. Respond to intrusions to minimize damage
5. Improve your security to help protect against future attacks

Other people advise protective measures such as:

1. All accounts should have passwords and the passwords should be unusual, difficult to guess.
2. Change the network configuration when defects become know.
3. Check with venders for upgrades and patches.
4. Audit systems and check logs to help in detecting and tracing an intruder.
5. If you are ever unsure about the safety of a site, or receive suspicious email from an unknown address, don't access it. It could be trouble. [15]

How To Test For The Adequacy Of Anti-Cyberterrorism And Anti-Cyber Crime Methods

One could make a good case for the futility of security testing. After all, there are so many points of vulnerability (holes) and so many sources of attack (crackers), that it would be impossible to test security measures exhaustively. However, you could make the same point in software testing in general. We know that we need to perform some level of security testing, so how do we get the most value for the time and effort expended?

In our security testing class module from RCS, we divide security testing into two distinct methods:

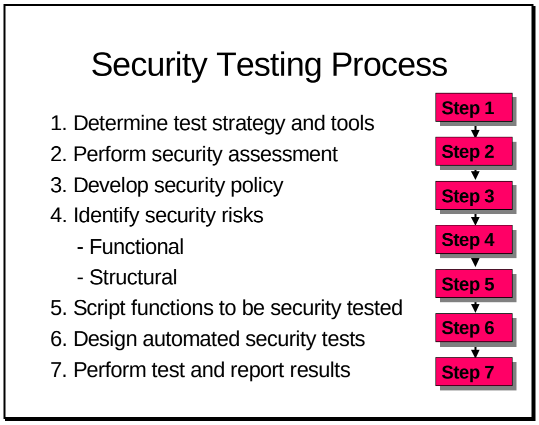
- **Verification methods** to review and assess that defined security methods and protocols are being followed by the organization.

[9] ibid
[10] ibid
[11] ibid
[12] http://www.techlawjournal.com/security/20001214.asp
[13] ibid
[14] ibid

[15] http://www-cs.etsu-tn.edu/gotterbarn/stdntppr/

- **Validation methods** to test the correctness and performance of the security measures that have been implemented.

Just like any other type of quality control methods, both of these views are needed to give a complete assessment of security levels in an organization.



Security Testing Process

1. Determine test strategy and tools
2. Perform security assessment
3. Develop security policy
4. Identify security risks
   - Functional
   - Structural
5. Script functions to be security tested
6. Design automated security tests
7. Perform test and report results

The following is the security testing process we teach in our training module on Testing Internet Security.

Step 1 – Determine Test Strategy and Tools

Like other forms of testing, in this step you define the scope of the test, who will perform it, what will be needed, which tools are available and most helpful. This can usually be accomplished in just a few hours with assistance from people knowledgeable in the security methods of an organization.

At this first step in the process, you will be faced with some basic decisions, such as, is it possible to perform an adequate level of security testing with manual methods or will we need to invest an automated security testing tools?

Step 2 – Perform Security Assessment

In the second step of the security testing process, you'll need to assess the current level of security. This includes examining that data is at risk, the value of the items at risk, who should be able to access security items, and the presence of security controls.

In addition, the security assessment should determine if the controls are effective and actually protecting the assets at risk. The security assessment should also determine if security measures have been tested and which intervals are they continually tested. The tasks in this step can include:

Obtain or develop the organizational cyber security strategy

Obtain or develop the organizational cyber security practices, including response measures
Review existing security tools
Interview those responsible for IT security

Step 3 – Develop the Security Policy

The third step in the security testing process is to develop a security policy that addresses responsibilities, assets at risk, acceptable and appropriate security measures, response in the event of the security break-in, and testing strategies for security.

Step 4 – Identify Security Risks

Functional risks include insuring that access rights have been correctly established, that authorization levels are correctly enforced, and that procedural controls (such as used in transactions) are correctly administered and are effective.

Much of the functional testing for security will resemble security tests for legacy and client/server systems, and can be performed using traditional test case methods.

Structural risks include insuring that firewalls are adequate, have been correctly implemented and maintained, insuring that network configuration is correct and networks have been correctly maintained. Also, a structural risk is the adequacy and correctness of encryption levels used for transferring data across the network.

A sample security risk assessment is shown at the end of this article.

Step 5 – Script Functions to be Tested

The fifth step in the security testing process is to design test scripts that will validate security measures based on the functional risks. This will require that points to be tested have already been established. The security test scripts can be based on scenarios that simulate transactions that are exposed to potential security breaches.

These would include scenarios such as testing access rights, authorization levels, and transaction controls.

For this type of security testing, traditional test cases and test scripts can be used effectively.

What Are the Sources of Security Breaches?

- Unprotected External Access
- Desktop Modems
- Disgruntled Employees
- Activists
- Sensitive Internal Data
- Web Servers on an Internal Network
- Unencrypted Information
- Weak Passwords

If the test must be repeated often, they can be added to automated test scripts and test cases that you may have currently in place, or you may choose to purchase a tool just for the purpose of automating security functions.

A test plan can be developed that focuses on the cyber security strategy and practices. The security policies and procedures serve the same function as requirements serve in a development project. If the security documents do not exist, that is the first finding of the security test and the test should be discontinued until they have been defined.

Step 6 - Design Automated Security Tests

A functional security test can be automated if you intend on performing them often. These types of tests can first be performed manually, and then recorded into automated test cases and test scripts.

Other types of automated security testing tools, such as vulnerability checkers can be used effectively without developing test cases in advance. Vulnerability scanners work by attempting to access the system in many different ways to test firewall effectiveness.

Step 7 – Perform Test and Report Results

This final step of the security testing process involves performing the designed test, whether manual or automated, and analyzing the results. These tests might need to be repeated until the expected level of security has been validated. In addition, some of these tests such as vulnerability scanning might need to be run on ongoing basis to detect security breaches.

The security test report should be detailed enough to describe clearly the findings and recommendations from the test. As with any other type of test reporting, test results should be objective and standardized to eliminate any political or cultural subjectivity. One of the best ways to keep test reporting consistent, objective, and standardized is to make it part of the overall Web testing process.

Conclusion

The cyberterrorism threat is real and not enough people are prepared to prevent or detect an attack. This impacts other organizations that may be well-prepared. Cyber security is a community issue. Like anything else, testing can only validate what has already been done. However, quality professionals can be important advocates for the awareness of IT security. By keeping our eyes open and applying effective techniques, organizations can go a long way to prevent attacks and recover quickly in the vent of an attack.

References

Report from the Institute for Security Technology Studies at Dartmouth College – Cyber Attacks During the War on Terrorism: A Predictive Analysis – http://globaldisaster.org/cyberattacks.pdf

National Infrastructure Protection Center – www.nipc.gov

Cyberterrorism Testimony Before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives by Dorothy E. Denning of Georgetown University - May 23, 2000 - http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html

Gilmore Commission Report - http://www.rand.org/nsrd/terrpanel/

Organized Crime and Cybercrime: Synergies, Trends, and Responses by Phil Williams
Professor of International Security Studies, University of Pittsburgh
http://usinfo.state.gov/journals/itgic/0801/ijge/gj07.htm

Rice Consulting Services, Inc.
P.O. Box 891284
Oklahoma City, OK 73189
405-793-7449
405-793-7454 FAX

Web Security Risk Assessment - Example

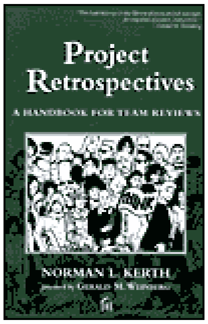
	Relative Value of impacted assets	Are controls in place?	Are detection tools in place?	Are the controls working?	Are the controls effective?	Are the tools working?	Are the tools effective?	Overall risk level
Unprotected External Access	5	1	5	3	3	1	1	19
Desktop Modems	3	5	5	5	5	5	5	33
Disgruntled Employees								
Activists								
Sensitive Internal Data								
Web Servers on an Internal Network								
Unencrypted Information								
Weak Passwords								
Totals								

Scoring Legend
High = 5, Moderate = 3, Low = 1, None = 0
No = 5, Somewhat = 3, Yes = 1

Book Review

Project Retrospectives

By Norman L. Kerth



Format: Paperback, 268pp.
ISBN: 0932633447
Publisher: Dorset House Publishing
Pub. Date: February 2001

★★★★★

Overview

One of the great “disconnects” in software projects is the lack of understanding and applying lessons learned. Many times a “post mortem” is scheduled as a cursory activity at the end of a project, but those kind of sessions often consist of blaming and complaining instead of constructive learning in a safe environment. After all, the name itself “post mortem” implies a study of something that is dead.

Project Retrospectives by Norm Kerth places an entirely new light on how to effectively and safely reflect on a recent project and not only learn from successes and mistakes, but to become a more solid project team for the next project.

I can testify after being in a project retrospective that is skillfully facilitated, there is a night and day difference from the traditional approaches. People are actually energized and management is involved and enlightened as well.

Who Will Benefit From This Book

- Project Managers and Leaders
- QA Managers
- Test Team Leaders
- Consultants
- Facilitators
- Business Analysts
- Software Developers

What I Liked About This Book

First, *Project Retrospectives* covers the topic completely in a very concise and readable way. You will find everything you need to know in this book in how to get started, how to be or find a facilitator, how to plan the retrospective, how to conduct the sessions – including a generous number of effective exercises, how to sell the concept of retrospectives to management and how to apply the lessons learned in an organization.

Second, I like the way that Kirth dealt openly and honestly with real world issues that surround project activities such as retrospectives that are often seen by management as “extras.” Kirth treats this topic with integrity and basically advises that if you can’t do the retrospective right, don’t do it at all – or at least wait until you can do it right. I never had to try to separate theory from practice as I read the book – it was all practical.

Finally, I enjoyed the clear train of thought throughout the book, along with specific examples and case studies. I never had to wonder where Kirth was going with a thought.

Scoring

Readability - 5
Breadth of coverage – 5
Depth of discussion - 5
Accuracy - 5
Credibility - 5
Organization - 5
Overall Score – 5

Major Topics

Chapter	Title
1.	Introduction to Retrospectives
2.	Anatomy of a Retrospective: A Case Study
3.	Engineering a Retrospective: Making Choices
4.	Selling a Retrospective
5.	Preparing for a Retrospective
6.	Retrospective Exercises
7.	Leading a Postmortem
8.	Postmortem Exercises
9.	On Becoming a Skilled Retrospective Facilitator
10.	After the Retrospective
	Index

Other Information

To read an interview with Norm Kirth, go to http://www.dorsethouse.com/news/interviews/intkerthv11n2.html#next

To read the forward by Gerald Weinberg, go to http://www.dorsethouse.com/news/excerpts/exprfore.html

To see a complete table of contents, go to http://www.dorsethouse.com/books/prcontents.html

Summary

It is time that we as software professionals make a ritual of reflecting on what we do and how effective we have been. In a profession where we try all too often to apply a single solution to many problems, the activity of project retrospectives can be a major force to improve the overall quality of projects. I highly recommend *Project Retrospectives* to project managers, consultants, QA analysts or anyone else wishing to be an agent of change in their organizations for higher software project quality.

Reviewer
Randy Rice, CQA, CSTE

Internal Certification of Software Testers

by Carl Chandler

Rice Consulting Services has been working with companies on creating their own internal certification programs for Software Testers and Software Test Engineers.

Companies are learning that this can be a great advantage to them. The way it works is simple. We sit down with you to learn about your company's current position in software quality/testing and where you want to be over the next few years. We then work with you to determine the type of training required to bring a person up to the desired target level. Next we work to compile a list of training courses to fit your specific needs. This includes customizing or developing courses specifically to meet those needs. It also includes developing tests at each desired level.

Attendees are put through the training courses and tested at pre-determined levels. Those who pass will receive a letter of completion given to both them and to their company.

What are the benefits of internal certification to the company?

- Complete control of training courses and content to fit your companies business needs
- Control of certification levels
- Control of continuing professional education requirements to maintain certification
- Control of cost; training, travel, testing, etc.
- On-Site training

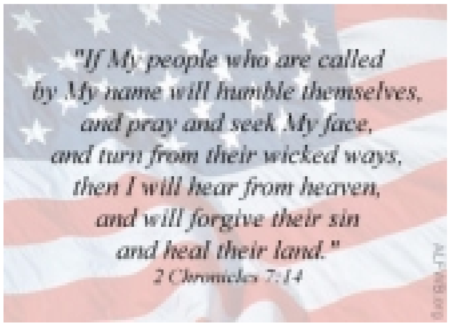
The alternative to internal certification is to have your employees certified through an external company. Some companies that provide this type of certification will offer courses for the employee to complete and upon completion they receive certification. Follow-up training through their company is generally required to maintain this certification.

Other companies will allow self-study and when your employee feels confident about the material, your company then pays a fee and the employee takes a test on a specific date at an off-site location. When the employee passes the tests they receive certification. The company then maintains the certification and the continuing education by each individual. These companies will determine the level of education required to maintain the certification and provide that each year for the following year.

What are the benefits of external certification?

- Responsibility for maintaining records is at the certifying company level
- The certification is universal. If the certifying company has a good reputation it can be of benefit to the employee when switching companies

These are both great options depending on the size of the company and the software quality/testing department within the company.



"If My people who are called
by My name will humble themselves,
and pray and seek My face,
and turn from their wicked ways,
then I will hear from heaven,
and will forgive their sin
and heal their land."
2 Chronicles 7:14

Rice Consulting Services, Inc.
P.O. Box 891284
Oklahoma City, OK 73189
405-793-7449
405-793-7454 FAX

Coming to Phoenix!
January 9-10, 2002

Process Documentation

by Suzanne Chandler

What I find to be most common in the companies I have worked with is the lack of documentation of their own company and departmental processes. Obviously they have processes because they are working to them every day to get a job done. However, when you ask two individuals how a certain job is done undoubtedly you will get two similar but different answers. So, when it is time to document the process requirements for a new application how do you begin?

One of the first items to look at in quality process documentation is to keep an eye toward the future. This includes the future of the business market and the future of the computer industry. Companies must not concentrate on a short-term solution. Making this mistake is very costly because most companies will outgrow the application before it is implemented.

Inevitably you are going to come across problems when attempting to document processes. It is important to go beyond the surface issues and identify the root causes of problems. This can be done by performing a root cause analysis using techniques such as facilitated brainstorming sessions with the people who perform the processes. Only when the root causes are understood can the right choices be made in process improvements and determining the best solution. The biggest mistake made here is substituting one technology for another. This method only attacks the symptoms.

Every company has a responsibility to their customer to constantly improve its product or service.

In our training course on Requirements we detail a process for defining, understanding, and solving problems:

- **Define the Problem**

  This is the first and foremost concern. If we can't state the problem, we can't even know where to begin.

- **Understand the Root Causes**

  Each problem has one or more root causes. Many times, the problem being seen is the result of the root causes, and is therefore a symptom, but not the core problem.

- **Identify the Affected People**

  Each problem will impact a given group of people. Each of these people will likely have different needs and concerns, which need to be considered in the solution.

- **Define the Scope of the Solution**

  The scope of the solution defines the boundaries within our control to solve the problem.

- **Identify Solution Constraints**

  There will often be barriers to solving the problem. Once identified, the barriers can be addressed instead of ignored.

Failure to identify the root problems before development begins or, even worse, after implementation can cause loss of dollars trying to resolve/rework the problem, lack of production, and perhaps even more detrimental to the entire process is distrust and dislike of the application by employees and/or customers.

It is key that you eliminate as much of the process failure, and scrap and rework as possible. Customers who find errors, even as simple as the spelling of a word, are often disappointed enough to seek business with other companies causing missed revenue for the company.

In our Software Testing Basics Course we teach that; “there is a definite economic impact of software testing. One economic impact is from the cost of defects. This is a very real and very tangible cost.

Most defects originate in requirements and design, but most of the testing effort occurs in a traditional ‘testing’ phase toward the end of the project. This is called the ‘big bang’ approach from the concentration of effort at one big phase. ‘Big bang’ could also describe the sound of the project as it fails.

The problem with the big bang approach to testing is that defects are not found until toward the end of the project. This is the most costly and risky time to fix defects. Some complex defects may even be impossible to fix.”

Being responsible for a budget, one of the most important lessons I learned from our Software Testing Basics Course is that “one of the most well-known facts about software defects is that the longer they go undetected, the more expensive they are to fix. Although research differs on the exact ratios, the general rule is 1:10:100.

That is, if a defect costs one unit (hour, dollar, etc.) to fix in requirements and design, it costs 10 units to fix in testing (system/acceptance) and over 100 times to fix in production. Sometimes the cost to fix a defect in production costs much more than 100 times the cost of fixing it in the requirements phase.

This cost of defects doesn’t even take into account the impact cost of defects. These costs could be attributed to lost revenue, reimbursements, fraud, lost customers, bad public relations, and litigation. In the case of safety critical systems, how can one put a cost value on a human life?”

The point of all of this is just to say that you need to begin at the beginning doing it right.

- Start with documenting and understanding your current processes.
- Take the time to develop new processes that include the best of what you do now with what you know is doable in the future.
- When looking toward the future get credible help from those in the industry (your market and the IT industry)
- Begin by testing early in the project and continue testing throughout the project – test your processes!

This may take money and time at the beginning but be patient it will save you even more in the end!

Next month, in part two of this article, the following questions will be answered:

- How can I get people to cooperate to write these processes?
- Where can I find a template or example of a good process?
- How much detail is needed in a process on a first cut?
- How many resources should be dedicated to developing processes?
- How do we maintain processes that change often?
- Who should be responsible for driving the process definition and maintenance efforts?

Rice Consulting Services’ Consulting Offerings:

Testing Assessments

Rice Consulting Services’ testing assessment is a quick and effective way for an organization to determine where they are in terms of software testing maturity. The assessment looks at three areas that are critical to testing:

• **Test organization** - Who performs testing, what levels of experience are present, and when testing is performed in the development/maintenance life cycle.

• **Test process maturity** - How well-defined, well-deployed, and repeatable the test process is, and whether it incorporates good testing management, practices, tools, and techniques.

• **Readiness** - An assessment of the organization's readiness to improve the testing process. This involves an assessment of the staff's testing awareness, testing skills, and motivation to change current practices.
The deliverable is a report detailing the assessment's findings, a recommended quality improvement strategy, and a plan for addressing the improvement needs identified. If the assessment uncovers the need for in-house skills training and consulting, we will include proposed training and consulting plans in the report. The report is typically about 15 pages in length.

In-House Software Testing Certification Programs

There is a lot of interest in certification programs for software development and software quality. There is also value to both the individuals being certified as well as the organizations that employ them. As you examine the various certification programs that are available, you need to ask:

- How recognized is the certification?
- What is the basis of the certification (i.e., what does it cover?)?
- How is the certifying organization accountable and responsive to its members?
- How closely do the certification criteria reflect the items important to your career and organization?
- What is the required investment to get and maintain the certification?
- What is the future for the certification program?
- What is the initial cost to your company to get certified?
- What is the annual cost to your company to retain certification?

After examining the above questions, some organizations have determined that the best certification program may be their own. One of the greatest advantages of an in-house certification program is that you can control the criteria, future and investment of the certification. As for objectivity, there are options that allow you to administer the in-house program while an independent organization verifies certification criteria.

Rice Consulting Services, Inc. has been working with several organizations recently to develop this kind of program. **We have extended certification training programs of 10, 15 and 20 days in length. These programs are tailored to your people, business, technologies and tools.** Participants range from experienced testers and QA personnel to people just entering the field.

This type of program makes the training effort more than a "one shot" event. People are tested at the end of each major topic area and are also evaluated by direct observation during exercises. The certification is normally determined by a combination of demonstrated proficiency during training as well as actual work experience. The certification criteria are defined by you, but we can help you with templates and examples.
Each in-house certification program is different. For details about how we can help you design and conduct an in-house certification program that is right for you and your organization, just call Carl Chandler at 405-414-6759 or email us at carlchandler@riceconsulting.com.

Rice Consulting Services' Course Offerings:

If you would like to learn more about the information covered in Carl's article we at Rice Consulting Services, Inc. offer an excellent course that will enhance your company's software quality process.

Build Your Own Course

– 2 – 20 days

Because all of our courses are designed to be modular, we can easily customize a course for you for presentation at your facility! A typical course day is 6 to 7 hours of instruction.

We provide a listing of all of our course modules at http://www.riceconsulting.com/build_your_own_course.htm. Simply select the modules you would like to have presented to your team. We provide a brief description of each module but if you would like to see more details, just click on the Module ID link. Upon submitting your course design, we will get a copy of your selections and will contact you by e-mail and phone.

Please note that our modules are not in alphabetical order. They are in order of popularity and typical presentation order. Specialized topics, such as Web-Based Testing, Client/Server Testing and E-Commerce Testing are found at the end of the list.

For those who hold professional certifications, such as the Certified Software Test Engineer (CSTE) and Certified Quality Analyst (CQA), each hour of instruction counts for one CPE credit. 40 CPE credits are required each year to keep these certifications current.

E-Commerce and Security Testing

– 1 day

This is a practical hands-on seminar to explore the deeper issues of testing e-commerce applications. A major aspect of testing e-commerce is security, so significant time is devoted to security testing. You will learn the terminology, the unique issues, and the process for testing e-commerce applications. As a result of attending this seminar, you should be able to understand e-commerce and security testing and have a working knowledge of designing and performing test cases for e-commerce.

E-commerce and Security Testing will help you become more comfortable and confident in dealing with e-commerce testing issues. You will emerge from this one-day session knowing how to develop a e-commerce application test strategy and plan. You will also have a working knowledge of how to perform a test of an e-commerce application.

E-Commerce and Security Testing is the second course in a three-part web testing trilogy. The first part is *Web Testing Overview* and the third part is *Testing Web Technology*.

Internet technology is a revolutionary resource that has the power to transform organizations, giving them a competitive advantage in today's global marketplace. E-commerce can help your company become more competitive and ultimately, more profitable. Learn the issues and processes for effectively testing this dynamic and profitable technology by attending this hands-on course.

Becoming an Effective Test Team Leader

2 days

This two-day session is designed for test leaders and test managers, people who expect to be in a test leadership role, or people who lead other test managers and test leaders. The main objective of this session is to teach you how to be the very best test manager and leader. This course also answers the question, "What does it mean to be the best?" There are many people functioning as test managers, but how many are really leading the team? In leading a test team, you must not only understand the basics of software testing, but you must also understand your own organizational culture. Once you understand your organizational culture, you might find that testers have a less than positive image. This session will discuss how to transform the image of testers from one of police to one of team members.

You will learn the terminology, process, and challenges of testing in the real world. Team-based exercises reinforce the concepts of facilitating team activities and performing leadership activities.

As a result of attending this seminar, you should have a good working knowledge of software testing and what it takes to design and conduct an effective test of software, regardless of the technology.

Becoming an Effective Test Team Leader will help you become more comfortable and confident in leading the testing effort in your organization. You will emerge from this two-day session knowing how to develop test cases and test plans. You will also leave with a knowledge of how tools can help you perform testing.

Sometimes people feel intimidated by the technical aspects of software testing and lack the confidence they need to be credible test leaders in their organization. Learn the issues and processes for effectively testing software by attending this hands-on course.

For more information on this course or one of our many other offerings please contact Carl Chandler at (405) 414-6759

Frequently Asked Questions

by Randy Rice, CQA, CSTE

Q: I took some courses from you in Minneapolis a few years ago, and I've been 'stopping by' your website periodically ever since. I really enjoyed the article "Everything I Need To Know About Testing I Learned From The Bible". I just read your article on user acceptance testing. I am working at a start-up company and trying to create a QA group (and process). I have gone through two iterations of UAT and have come to the conclusion that our users do not have a good understanding of what they are supposed to be doing (my fault - I didn't realize their level of expertise in this area).

I have been considering two options: write

UAT scripts for them to follow; or work with their management and develop scenarios/use cases for them to use. The users are primarily internal sales people who don't have a lot of time to spend on testing - perhaps 1 to 2 hours at most. That is why I felt scripts would be useful. However, there are drawbacks with scripts – it really narrows what they will be doing, and may not capture their 'real world' activities and actions.

What would you recommend? I have also considered getting a copy of their SOPs and creating scenarios for my test team to go through, and skip the UAT altogether, but I don't like that idea because I feel that we need the user input.

A: It sounds like you need a method for UAT that is a lighter touch than the method I teach. I would suggest developing a list of tasks for them to perform on the application and observe haw they perform them. I know that this sounds a lot like a usability test, and in many ways it is. However, the key is to offer guidance without being restrictive or overwhelming. By identifying the tasks only, you let the users decide how they will do them and let them use their judgment on evaluating results. I would also limit the test sessions to 2 hours or less. Also, consider how many users you have testing at once. In the real world, if they are working together, you may want to pair them up. Otherwise, you may want to have them work alone
during the test. In any event, you will want to be there to facilitate and observe.

Q: As always I am looking for your help and expertise. Please advise on definition for "Data and Database Integrity Testing". Thank you very much

A: When discussing data integrity, you are concerned that data stays in a correct state. This includes the values stored in files and tables, as well as the relationship between data, such as parent/child relationships. Data integrity testing (and database integrity testing) validates that the data stays correct and that measures are taken to recover and restore data if corruption does occur. Therefore, some tests may be static, such as reviewing procedures for backup and recovery, while other tests may be dynamic and validate edits and data maintenance, as well as backups and restores. It's always wise to test that you can restore the data that has been backed up!

Q: Thanks for emailing me the information on the October Newsletter. I particularly enjoyed the review of the book on 'Debugging'. I will be purchasing a copy of this book next week. I downloaded the copy of chapter 2 you have a link to and really enjoyed reading the case histories. I am studying for a CSTE exam and would like to read more case histories. Do you have any other sources for case histories and/or case studies?

A: Thanks! I glad you enjoyed the book chapter. As you can tell, I think it is a great resource for testers and developers to understand about defects. If you are looking for other case studies, a good choice is "Fatal Defect" by Ivars Peterson. Another book is "Computer-related Risks" by Peter Neumann. There is also a book that is out of print, but still very good on the topic by Leonard Lee called "The Day the Phones Stopped." I found a copy by doing a web search.

I wish you the best on your upcoming CSTE exam!

Q: I checked your glossary for the term but couldn't find the term "smoke test". Could you elucidate?

A: Thanks for writing. As far as I know the term "smoke test" is used to refer to a screening type of test that exercises basic functions, such as navigational objects, but stops short of testing business rule functionality. One anecdote I have heard references tests of closed ventilation systems to find leaks by pumping smoke through them and finding air leaks, so perhaps that is where the term originated. Smoke tests in the systems context are helpful in validating that basic standard (generic) functionality works and is sometimes a first candidate for test automation.

Photo available at http://attacked911.tripod.com

New York Mayor Rudolph Giuliani spoke with President Bush from the scene of the latest plane crash:

"He said, `New York City is really being tested. It's a shame.' I said, `Mr. President, New York City is up to the test."'

God bless New York City and God bless America.

Links…

To go with Randy's article this month on *The Threat of Cyber Terrorism*, we also have these links on security that are outstanding resources.

The Encyclopedia of Computer Security - Must See!

http://www.itsecurity.com/defaultie5.htm

Antionline.com – Hackers know the weaknesses in your system. Shouldn't you?

http://www.antionline.com/

COAST-- Computer Operations, Audit, and Security Technology -- is a multiple project, multiple investigator laboratory in computer security research in the Computer Sciences Department at Purdue University. This site contains a hotlist of many other security sites.

http://www.cerias.purdue.edu/coast/coast.html

Notable Quotes…

"The best way to predict the future is to invent it."
-Alan Kay

"The problems that exist in the world today cannot be solved by the level of thinking that created them."
-Albert Einstein

"I cannot say whether things will get better if we change; what I can say is they must change if they are to get better."
-G. C. Lichtenberg

"One's mind, once stretched by a new idea, never regains its original dimensions."
-Oliver Wendell Holmes

"If we will not be governed by God, then we will be ruled by tyrants."
-**William Penn**

"Poor is he who works with a negligent hand, but the hand of the diligent makes rich."
- The Bible - Proverbs 10:4

Photo available at http://attacked911.tripod.com

Rice Consulting Services, Inc.
P.O. Box 891284
Oklahoma City, OK 73189
405-793-7449
405-793-7454 FAX

Coming to Phoenix!
January 9-10, 2002

December 2001 Issue:

- **Dealing With the Intimidation Factor in Software Testing**
  by Randy Rice, CQA, CSTE
- **Test Tools**
  by Carl Chandler
- **Process Documentation, Part II**
  by Suzanne Chandler

Coming to Phoenix!

January 9-10, 2001

Rice Consulting Services, Inc., *a world recognized leader in Quality and Testing Training.*

To present to you a Two-day course in Becoming an Effective Test Team Leader

Log on to http://www.riceconsulting.com/phoenix2002.htm *to learn more about the course and to register.*
Look for early-bird incentives!

This certificate worth _____ CPE credits* towards Certified Software Test Engineer Continuing Professional Education through the Quality Assurance Institute.

*Category E - Self-Study Courses Activities designed to improve your proficiency in CSTE skill areas as defined in the *Common Body of Knowledge* may qualify for CPE credit up to a **maximum of 20 credits per yea**r. Qualifying activities include: Professional memberships that offer self-study education regarding quality assurance within information technology. It's not the membership that earns the credit, but the study materials provided by the membership.

To redeem complete the following information and submit to the Quality Assurance Institute at the time of reporting CPE credits.

Name: ____

CSTE/CQA Certification Number: _____________________
(circle one)

Email Address: _____________________________________

Credits available to members of The Software Quality Advisor only. To become a member of The Software Quality Advisor sign-up at http://www.riceconsulting.com/SQAdvisornew.htm

Rice Consulting Services, Inc.
P.O. Box 891284
Oklahoma City, OK 73189
(405) 793-7449 / (405) 793-7454 Fax
e-mail rcs@telepath.com
http://www.riceconsulting.com