Top 10 Cyber Security Issues for 2008

Information technology systems are the underpinning of our economy and nation's security. Most of these systems rely on the Internet for communications. Security issues abound and many individuals become overwhelmed and have a difficult time assessing those issues which pose the greatest threat. The following list identifies the top ten cyber security issues for 2008.

1) **Preparation for Cyber Warfare**
Net-Centric Warfare is a reality and is continuously evolving. As computer technology has become increasingly integrated into modern military organizations, military planners have now come to see it as both a target and a weapon. We need to lead the world in offensive and defensive cyber warfare capabilities. In 2007 the world saw the first nation to nation cyber war between Russia and Estonia.

2) **Protecting Our Critical Infrastructure**
Everything from our national power grid to our cars to our air traffic control system uses software. Software is produced with quality issues, performance issues, and security issues that can be exploited by those who wish to do us harm or negatively impact the economy. It only takes one error to create a catastrophic event like the Northeast Power Outage.

3) **Data Vulnerability and Protection**
The world produces about 2 exabytes of unique information per year and digital storage is by far the largest storage medium. Paper accounts for only about .003% of this. Our ability to protect our digital assets relies on our ability to thoroughly test systems software. *80% of the data is not encrypted.*

4) **Software Bugs are a National Security Issue**
While acknowledging that software makers continue to release buggy products, Richard Schaeffer, deputy director of the National Security Agency, stressed that publicizing vulnerability without warning and before a patch has been created could potentially threaten US computing systems. Schaeffer's comments echoed those of presidential cyber security adviser Richard Clarke, who spoke at the Black Hat Security Briefings in Las Vegas. Clarke told attendees that finding vulnerabilities in buggy software is important; but properly handling the disclosure is critical.

5) **Economic Costs of Software Bugs**
According to a 2002 Study by Silicon Valley Firm vnunet.com, software bugs are costing the US economy an estimated $59.5 billion a year. This study found that more than half the costs are carried by software users and the remainder by software developers and vendors. In the automotive and aerospace study, NIST found that about 60 per cent of firms had experienced "significant software errors" in the previous year. The total cost from inadequate software testing was estimated to be $1.8 billion.

6) **Software Bugs Can Cost Lives**
A poorly programmed ground-based altitude warning system was partly responsible for the 1997 Korean Air crash in Guam that killed 228 people, and, in another case, faulty software in anti-lock brakes forced the recall of 39,000 trucks and tractors and 6,000 school buses in 2000.

7) **Alternative Devices**
Game platforms like the X-Box or Play Station have high powered processors and are connected to our networks and the internet. These devices do not have firewalls or anti-virus protection. Exploiting these high end processors in a distributed denial of service attack would create a cyber attack like none we have ever seen before.

> ***Definition:*** *Denial of Service (DOS) Attack--An attack directed towards a service, computer system or network with the objective of making it inaccessible to legitimate users. There is also a distributed denial of service attack (DDOS).*

8) **Foreign Software Influence**
A significant portion of our country's computer systems are built using foreign supplied components and even software. The size and complexity of the software makes manual inspection for malicious code unrealistic. A foreign power could place malicious code in components that find their way into our defense or business systems. We have no way of knowing at this point, which leaves our current strategy to be "In Code We Trust."

9) **Protecting Our Financial Infrastructure**
The global economy is changing through the new information networks. In the near future, most businesses deals will be arranged via the electronic marketplace. Disruption of the electronic marketplace would have catastrophic consequences on a scale that, for a time, will cripple the global economy.

10) **Identity Theft – A Terrorist Tool**
Through human error, deception, and software vulnerabilities millions of identities get stolen each year. While most of the thefts are for financial gains, consider the possibility that a terrorist could assume the identity of a U.S. citizen without ever raising a suspicion on a credit monitoring report. Why would they do this? So they can come into and out of the U.S. without undergoing scrutiny associated with foreign visitors.

" If you do not have up-to-date security measures
- then you should have a GREAT ATTORNEY!"
—Ralph Parton, Ph.D.

As we rapidly approach 2008 business, government and industry needs to take a very hard look at cyber security. The nation's critical information infrastructure remains highly vulnerable to premeditated attacks with potentially catastrophic effects. Thus, it is a prime target for criminal activities as well as cyber terrorism. Security indicators and trends within organizations large and small clearly reflect rapid growth in the rate of cyber attacks. The time to address these issues is now!

References & Sources

1. **Preparation for Cyber Warfare**
   - **Spy-Ops Counter-Terrorism Certificate Program**
     www.spy-ops.com
   - **The Technolytics Institute Research Study and Directions Magazine Article**
     http://www.directionsmag.com/article.php?article_id=562&trv=1
2. **Protecting Our Critical Infrastructure**
   - **The Technolytics Institute Research Study and Directions Magazine Article**
     http://www.directionsmag.com/article.php?article_id=2184
   - **Software Flaw Contributed to Northeast Blackout**
     http://www.securityfocus.com/news/8016
3. **Data Vulnerability and Protection**
   - **PGP Supports Data Protection**
     http://www.darkreading.com/document.asp?doc_id=120782
   - **Data vulnerability is a systemic problem**
     http://www.azcentral.com/arizonarepublic/viewpoints/articles/0521monahan0521.html
   - **The Technolytics Institute 2001 Testimony before the Congressional Privacy Caucus**
4. **Software Bugs are a National Security Issue**
   http://www.pcworld.idg.com.au/index.php/id;1888189123
   http://www.esecurityplanet.com/views/article.php/3562191
5. **Economic Costs of Software Bugs**
   http://www.rti.org/newsroom/news.cfm?nav=341&objectid=DA7FBFE6-4A4F-4BFD-B77E0FA3C04D9E22
   http://blog.eweek.com/blogs/baseline_security/archive/2006/10/25/14158.aspx
6. **Software Bugs Can Cost Lives**
   http://208.37.5.10/fsd/fsd_may_july00.pdf
   1. http://russia-from-the-inside.blogspot.com/2006/11/software-bugs-lead-to-deaths-from.html
7. **Alternative Devices**
   - **The Technolytics Institute Research Study and Presentation at the 2005 Security Summit**
     http://www.protect-me.com/corporate_security.html
     http://news.com.com/Employee+gadgets+pose+security+risk+to+companies/2100-1029_3-5954642.html
8. **Protecting Our Financial Infrastructure**
   - **The Technolytics Institute Research Study and Presentation at Wharton**
   - **Technolytics Published Articles in Eye Spy Magazine in London**
     http://www.directionsmag.com/article.php?article_id=593
9. **Identity Theft – A Terrorist Tool**
   http://www.directionsmag.com/article.php?article_id=2033

CONTACT

Spy-Ops
4017 Washington Road—MS #348
McMurray, PA 15317

P 888-650-0800
F 412-291-1193
I www.spy-ops.com

About the Author:

Kevin G. Coleman is an international security and intelligence consultant with Technolytics and has regularly featured articles in Directions Magazine and International Intelligence Magazine covering homeland security, terrorism, security and intelligence worldwide. For six years he served as a science and technology advisor to the nation's leading research and development center that service the U.S. Department of Defense, Department of Homeland Security and the Intelligence Community. Additionally, he testified before Congress on Cyber Security and Privacy.