Alcatel·Lucent

Changing Faces of Cyber Crime -- Protecting the Organization from Inside Threats

Dr. Jim Kennedy, NCE, MRP, MBCI, CBRM, CHS-IV

Best of NY 2008

March 2008

•Defence in Depth

•VPNs

•SPAM Filtering

•Firewalls

•Access Control Lists

•Intrusion Detection

Alcatel·Lucent

Alcatel·Lucent

NEW FACES OF COMPUTER CRIME

Insider attacks account for as much as 80% of all computer and Internet related crimes

70% of attacks causing at least $20,000 of damage are the direct result of malicious insiders

Alcatel·Lucent

AGENDA

➢ Insider Threat – A big problem

➢ Basic types of RISKS

➢Where do threats come from

➢Who are insider threats

➢Statistics

➢ Costs

➢ Types Encountered

➢ What Can be Done

➢ Recognized Best Practices

➢ What others are doing

➢ Questions

Alcatel·Lucent

FROM THE US SECRET SERVICE – National Threat Assessment Center

The greatest information security threat facing your organization is in your office right now. It has the ability to bypass the physical and logical controls you've put in place to protect the perimeter of your network and has already obtained credentials to access a significant portion of your infrastructure. What is this threat? It's the often underestimated insider threat -- the risk that your users will violate the trust you've placed in them not to conduct malicious activity on your network.

What can you do to protect yourself? First, you must understand the nature of the threat.

Alcatel·Lucent

TYPES OF RISKS – COMPROMISE OF DATA/BREAKING THE LAW

February 2008 -- Dallas-based Tenet Healthcare Corp. sent out notices to about 37,000 patients informing them about the potential compromise of their personal and financial data. The warning came after a former data processor at a Tenet bill-processing center in Frisco, Texas, was arrested last month and subsequently pleaded guilty to five counts of fraudulent possession and use of identification information stolen from Tenet. At the time of his arrest, the suspect had identity information belonging to about 90 patients in his possession.

Alcatel·Lucent

TYPES OF RISKS – Loss of Identities/Financial Fraud

In another case a help desk employee (a contractor) stole the identities of up to 30,000 people by using confidential passwords and subscriber personal information from his firm's customers such as banks to access and download credit information. The breach went undetected for more than two years and enabled the employee to obtain credit cards in the names of people whose identities were stolen.

Alcatel·Lucent

TYPES OF RISKS – Unintended exposure of identity information

What happened?

On March 26, 2007, the spouse of a US Sales colleague loaded unauthorized personal software onto a major pharmaceutical company's laptop for the purpose of accessing a "peer to peer" file sharing network. That software gave other users of the file sharing network access to approximately 2300 files in the "My Documents" section of the colleague's laptop, including names, social security numbers and in some instances, addresses, home and/or cell phone numbers and bonus data for approximately 17,000 present and former colleagues. After learning about the unauthorized software on April 18, 2007, the company took action the same day to retrieve the laptop and disable the software. (17000 X 200 = $3,400,000 credit theft insurance)

What data was exposed?

The names, social security numbers, and in some instances addresses, home and/or cell phone numbers and bonus data, concerning approximately 17,000 present and former company colleagues were accessible to users of the "peer to peer" file sharing network.

Alcatel·Lucent

TYPES OF RISK -- LOSS OF INTELLECTUAL PROPERTY

A scientist who admitted he stole $400 million in intellectual property from his former company.

The former employee who worked as a research chemist for a major petrochemical company for 10 years before accepting a job with competitor in October 2005, pleaded guilty on Nov. 13, 2006, to stealing trade secrets.

The individual faces a maximum prison sentence of 10 years, a fine of up to $250,000 and restitution. He admitted downloading 22,000 sensitive documents and viewing 16,706 more in the company's electronic library.

That made him the database's most active user, according to prosecutors. After months of accessing the intellectual property unimpeded, the employee informed the company that he was leaving the company in 2005. The company noticed his unusually high data-access rate within the library after he gave notice and contacted the DOJ.

After the employee left the company, he transferred 180 critical documents to a competitor's owned laptop after switching jobs.

Alcatel·Lucent

Additional Breaches Encountered

➤ Small telecom carrier's employees were providing PIs, for remuneration, call records on specific individuals – logging might have helped

➤ Banks systems programmer rounding deposits and placing $$ into an off-shore account.

➤ Hospital employee disclosing information regarding a celebrity's injuries following an accident

➤ Laptop stolen from inside a car with information regarding terminally ill patients taken inappropriately to do work from home

➤ E-mail of AIDs patient list sent incorrectly to law office instead of a clinic

Alcatel·Lucent

Hacker and Organizational Culpability in Reported Incidents of Compromised Records, 1980-2006

Legend:
- □ Unattributed
- ▨ Attributed to Hacker
- ■ Attributed to Organization

Alcatel·Lucent
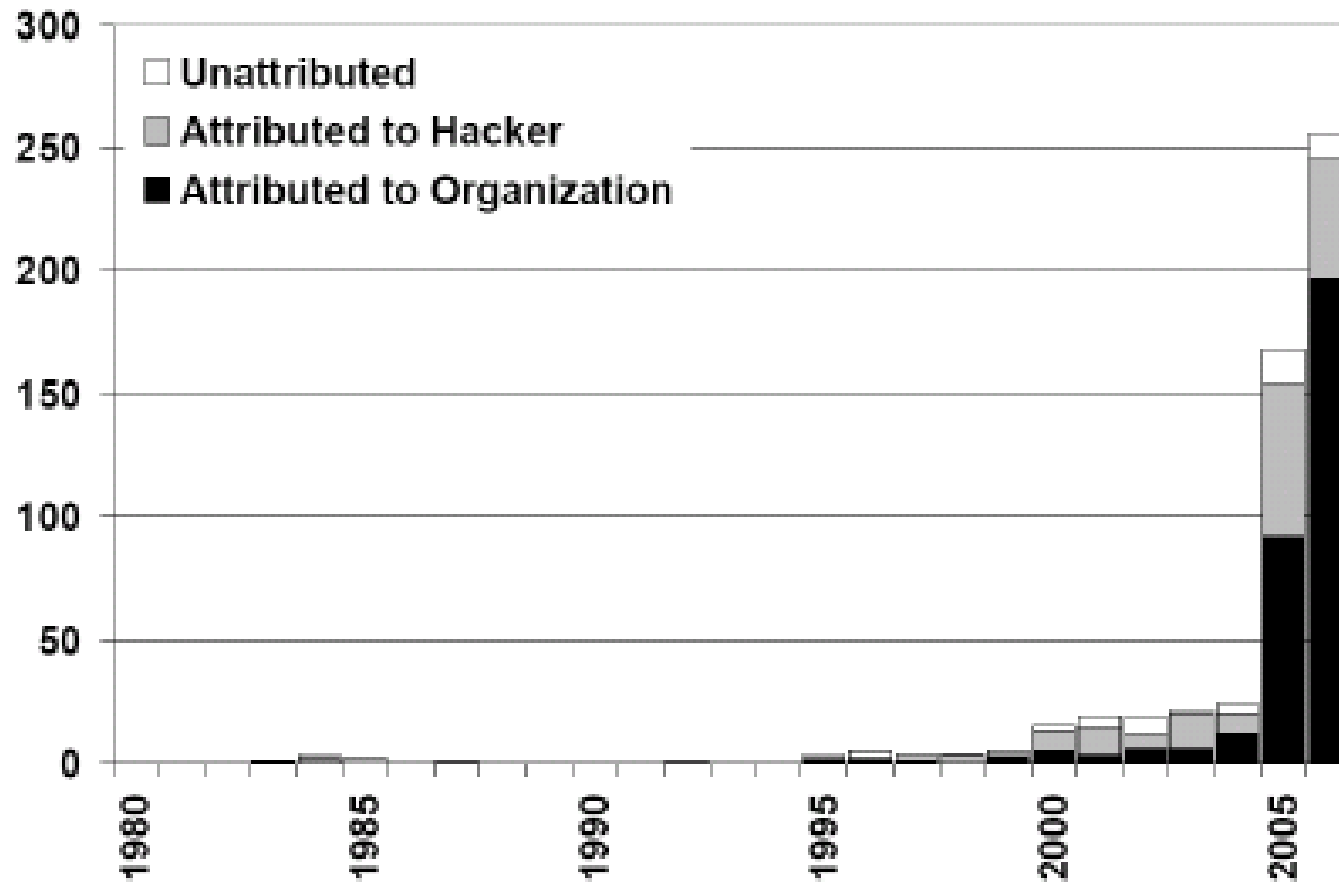
WHO ARE THE PERPRETRATORS

Individuals with Malicious Intent to Cause Harm

➢The IT Expert with a Hacker Mentality

➢ The Dissatisfied or Disgruntled Employee

➢ The Terminated or Demoted Employee

➢ The Fraudster Motivated by Financial Gain

➢ The Employee Who Wants Unauthorized Access to Information

Individuals Who are Inattentive (Non-Malicious Intent) or Complacent

➢ The Tech-Savvy Employee Who Gets Around Security Measures

➢ The One Who Just Doesn't Pay Attention

- IT Staff

- Non-IT Staff

➢ The Untrained New Guy

➢ The Employee without Adequate Training

Alcatel·Lucent

WHAT ARE THE ACTUAL THREATS ?

Threats can be classified in one of four areas:

➢Malicious/disgruntled employees: these are current and recently terminated employees have a desire to do damage to the IT infrastructure or critical information because of a grievance they have against the organization

➢Unintentional exposure or breaches: these occur where employees put the IT infrastructure and critical information at risk by installing unauthorized software, opening virus-infected email attachments, succumbing to social engineering attacks, spilling coffee into a server, releasing sensitive information to friends or relatives, and etc.

➢Corporate espionage: where hackers, thieves or spies recruit and sometimes pay employees to steal critical data or damage critical IT infrastructure

➢Dishonest insiders: those who abuse employee privileges to their own personal gain or satisfaction

Alcatel·Lucent

TOP FIVE INSIDER THREATS

> **PEOPLE**

THREAT 1: Malicious Employees (with or without IT knowledge)

THREAT 2: Inattentive, Complacent or Untrained Employees

THREAT 3: Contractors and Outsourced Services (IT and non-IT)

> **PROCESS**

THREAT 4: Insufficient IT Security Compliance, Oversight, Authority and

Training (Policies, Procedures, Practices???)

> **TECHNOLOGY**

THREAT 5: Pervasive Computing— Technology is Everywhere and Data is on

the Move

Alcatel·Lucent 🔵

SOME STATISTICS

➢Only 17% of the insider events studied involved individuals with administrator access

➢87% of the attacks used very simple user commands that didn't require any advanced knowledge

➢30% of the incidents took place at the home of the insider using remote access to the organization's network

➢Most insider events were triggered by a negative event in the workplace

➢Most perpetrators had prior disciplinary issues

➢Most insider events were planned in advance

➢Total costs averaged $182 per lost customer record, an increase of 30 percent over 2005 results. The average total cost per reporting company was $4.8 million per breach and ranged from $226,000 to $22 million.

Alcatel·Lucent
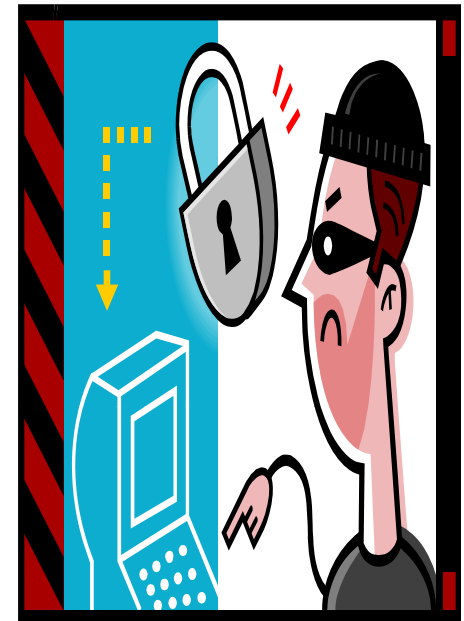
A FEW MORE STATISTICS

The new Ponemon report helps document the greatest insider threats. US IT respondents responded in the following percentages when asked about what constitutes the greatest risk (each respondent was allowed two choices):

➤Careless employees (34%)

➤Negligent employees (32%)

➤Temporary employees (29%)

➤Disgruntled employees (21%)

➤Terminated employees (19%)

➤Partners (16%)

➤Privileged users (12%)

➤System administrators (11%).

Alcatel·Lucent

COSTS OF SUCH INSIDER THREATS

The insider threat poses serious risks that have the capacity to cost companies huge sums in law suits, regulatory penalties, lost business, intellectual property infringement as well as unquantifiable damage to that most valuable of assets - reputation.

Insider Computer security attacks can cost as much as $10 billion a year. An attack can damage data integrity, confidentiality or availability – NYS Department of Health.

Alcatel·Lucent

WHAT INSIDERS THEMSELVES HAVE SAID (a confessions survey conducted by RSA in Washington and Boston)

➢ 35% felt the need to work around established security policies to get their job done

➢ 63% send work documents to personal e-mail addresses to access them from home

➢ 45% download personal software onto a company computer

➢ 56% have accessed their work e-mail via a public wireless hotspot, such as Starbuck's

➢ 34% have held a secured door open for someone at work that they did not recognize

➢ 39% have lost personal data-bearing device – 72% did not report immediately

➢ 46% share passwords with co-workers

➢ 51% copy confidential information on USB stick

Alcatel·Lucent

WHAT CAN BE DONE ?

➢DEALING with the:

- Regular Employees

- Disgruntled Employees

- Contractors

- Malicious Employees

➢Policies provide a modicum of protection.

➢Education, Training & Controls

➢BEST PRACTICES

- People

- Process

- Technology

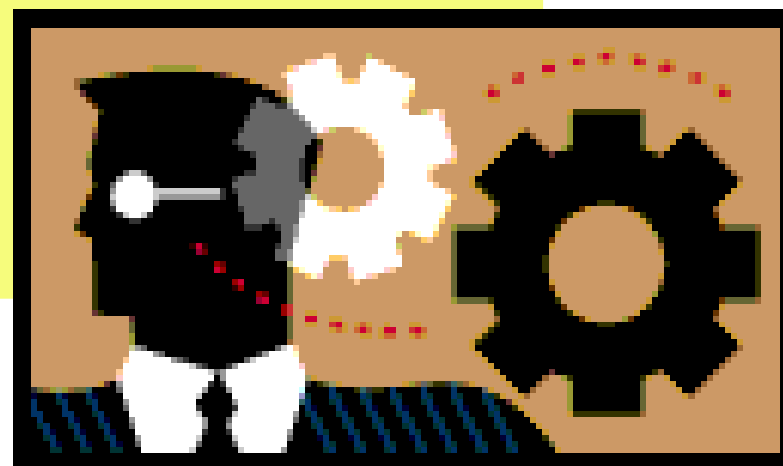➢What Has Worked for Other Organizations

Alcatel·Lucent

Did you Know?

"Plans are only good intentions, unless they immediately degenerate into hard work."
-Peter F. Drucker

Alcatel·Lucent

DEALING WITH REGULAR EMPLOYEES AS THREATS

➤ **The Complacent Employee**: Some employees' jobs are extremely routine. The job might consist of entering data into a database that contains patient medical information. As each month on the job passes the task of data entry becomes more rote and mundane. By the end of a year or so the employee may not fully appreciate what could happen if data is entered incorrectly or if a mistake leads to the leaking of a patient's medical information to the public. *(Think about job rotation if at all possible)*

➤ **The Inadequately Trained Employee**: For a very large corporation which has business units geographically scattered across the globe it is quite possible that training and awareness practices are inconsistent across business operations. Many employees who use technology regularly in their personal lives may not have a proper appreciation for security risks. These are the very same employees who do not quite understand the value of keeping their anti-virus signatures up-to-date.

➤ **The Inattentive Employee**: Many employees may not realize the risks that go along with having access to state IT resources. Moreover, with the lines blurred between home use of technology and use in the workplace, some employees may not have a realistic appreciation for the risks to the network that can result from checking a personal email account or just doing some random Internet surfing while on the job. Employees also are operating in a network-centric environment, which creates the possibility that a virus downloaded to one computer could infect a myriad of other computers connected to the same network.

Alcatel·Lucent

DEALING WITH THE UNHAPPY OR DISGRUNTLED EMPLOYEE

Dealing with the Disgruntled Employee:

➢**What's in Their Background?** Background checks of all job candidates, including interns and contractors, can identify those with inappropriate backgrounds and criminal records. A record of acting inappropriately or using questionable judgment should also prevent their hiring in the first place. A credit and financial background check can aid in the identification of candidates in financial difficulty. They could have an incentive to use IT to defraud your organization or your customers especially if the position has financial responsibilities or access to financial IT systems.

➢ **Vigilance Pays Off:** Management should be aware of the warning signs of a disgruntled employee who might cause damage with or to your organization's IT resources.

➢ **Open Communication Channels Between Employees and Management**: A method for employees who witness or know of a disgruntled employee with ill-intended plans to report them can act as an early-warning system to management. Also, providing employees an official channel for the expression of grievances may prevent them from taking their anger out on the organization.

Alcatel·Lucent Ⓐ

(continued)

➤ **Watch Employees with Problems:** For problem employees, managers may consider coordinating with state IT staff to monitor their access to email, the Internet and state IT systems.

➤ **Audits are Important:** Regular and ongoing audits may identify ill-intended behaviors of employees that management may not immediately recognize as disgruntled. Audits can include the review of access, activity and facilities logs.

➤ **Have a Well Thought Out Exit Strategy:** Employees who resign or are terminated may take one last swipe at their employer through sabotage or data theft. A formal and thorough exit process can prevent such occurrences. A process which includes cutting off access privileges before an employee is terminated or immediately after an employee resigns if the employee appears to be disgruntled and escorting an employee out of the office is very important.

     Alcatel·Lucent *A*

DEALING WITH CONTRACTORS

➤ **Same Rules Apply to Contractors:** Ensure that background checks, IT security training, and roles-based access policies apply to contractors. Specifically, the company should perform background checks on contractors to ensure that a contractor's company is not relying on an incomplete or dated background check.

➤ **Make Sure Contracts Include IT Security- Related Provisions:** To ensure that IT security policies and procedures are legally binding, all contracts for services should include language to ensure contractor compliance. Other provisions should address security measures for data handling and audits. In the event of a security incident the contract should clearly address the rights and responsibilities of each party and provide the company with termination rights in the event of a particularly egregious security event. A contractor should be required to notify the company immediately upon the occurrence of a security breach.

➤ **Have all Contractors Sign:** All contractors who have access to corporate IT resources should be required to sign a non-disclosure agreement in addition to an acknowledgment and agreement to follow all IT security policies and requirements.

➤ **Regulatory:** For companies that must comply with HIPAA, PCI, SOX and etc. they should have business agreements with any contractors, even those working on facilities related projects, who could have access to personal or customer information.

Alcatel·Lucent Ⓐ

DEALING WITH THE MALICIOUS OR CRIMINAL EMPLOYEE

➢**Dealing with the IT Expert with a Hacker or Criminal Mentality:** Note that, with this type of insider, their lack of ethics and moral underpinnings may be no match for typical security measures, such as roles-based access and security awareness training.

➢ **Trust, but Verify:** Diligent monitoring and auditing of employee access to IT systems, email and the Internet may turn up abnormalities that are warning signs of such activity.

➢**Severe Consequences:** Deal with such offenders in a swift and severe way, making consequences (including criminal charges) known and enforced.

➢ **Applicability of Criminal Laws:** Review state and federal criminal laws regarding computer trespass and unauthorized access for applicability to employees and then educate employees regarding their responsibility to abide by any such laws.

➢ **Focus Ethics:** Training in ethics, especially for those with greater access privileges, may play an emerging role in this area. It could serve as a reminder of the importance of integrity and the level of responsibility that accompanies IT access privileges. This training would focus on identifying and analyzing ethical problems that system administrators and others may face in carrying out their day-to-day duties.

Alcatel·Lucent

POLICIES CAN PROVIDE A MODICUM OF PROTECTION (for the breaches caused by unsuspecting personnel)

The most effective way to utilize security controls to protect against the internal threat is to implement a multi-layered strategy right from the beginning. One level of protection is to develop policies that address process, people's behaviors and technologies.

Examples of policies that target internal breaches are:

➢ Policies governing the acquisition and use of external removable media such as floppy disks, flash drives, USB/Firewire hard drives, CD burners, and etcetera. The source of many internal breaches have occurred when insiders copy company data to removable media, or bring in removable media from which they install programs or simply upload critical data from the IT infrastructure.

➢ Policies governing e-mail attachment. Numerous internal security breaches and subsequent loss of critical employee or customer information have occur when someone on the inside opens infected attachments, or has sent confidential company or customer personal or financial data outside of the organization's IT infrastructure network using an email attachment.

Alcatel·Lucent Ⓐ

POLICIES (continued)

➢ Policies that restrict printing of critical or restricted information or data. If insiders are unable to send or take company data in electronic form the next most used method is to print the information take the hard copy.

➢ Policies regarding downloading of information or programs. Many unknowing security breaches are caused by those on an IT infrastructure that were downloading information from the web that happened to contain malicious code, which then provided remote attackers, thieves, and spies with a way into the IT infrastructure and all that it affords.

➢ Policies about "need to access" privileges. Many security breaches have come about by allowing employees more access to critical information than was actually needed to perform the duties of their position.

➢ Policies about placing critical employee, customer, or company critical data or information on laptops. Many of the most publicized data breaches over the last three years have occurred due to laptops being stolen which contained information which should not have been allowed outside of the organization's protected confines.

➢ Information Classification and Handling policies dictating classification of data and defining its access, use, and protection is also critical.

Policies must be enforced and reinforced by education and controls

Alcatel·Lucent

EDUCATION & CONTROLS

Simply creating policies directed at internal threats is not enough. Once created an organization must ensure that those policies are effectively implemented and controlled with activities such as:

➤ Distribute the completed policies and ensure that users sign off on having received, read, and understood them and their individual responsibilities under those policies

➤ Reinforce the written policies with employee training to prevent unintentional breaches (e.g., educate users on safe web surfing practices, the dangers of opening unknown e-mail attachments, to importance of good password administration, etc.)

➤ Bolster the policies with technological controls (ISO-17799) whenever possible (e.g., password aging, access log reviews, internal IT audits, and etc.)

➤ Awareness is important (MBWA) !

Alcatel·Lucent

BEST PRACTICES

➤ People

➤ Process

➤ Technology

Alcatel·Lucent
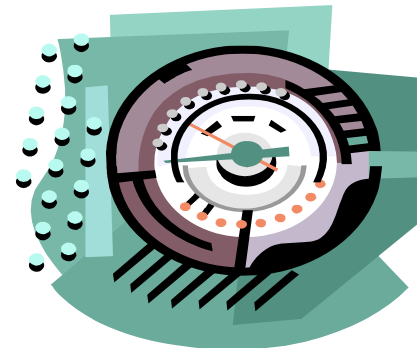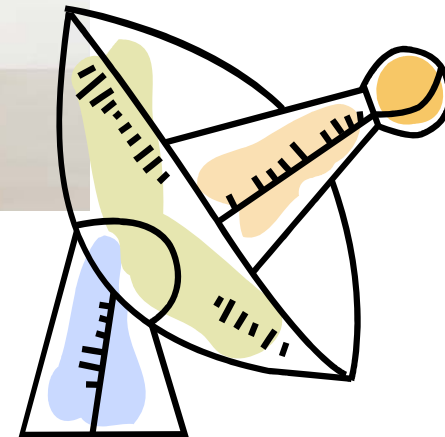
BEST PRACTICES - PEOPLE

- **Require new hires to go through a security orientation.** Have employees review and sign a policy concerning the acceptable use of company IT resources. In addition, an orientation program should include a review of the threats; a specific list of do's and don'ts to protect corporate information, passwords and physical security; and what to do (and whom to contact) if an employee discovers a security violation.

- **Do not overlook the sensitive data on common office peripherals**, such as copiers and printers. When these products are used, the memory of that use remains in the machine, sometimes for years. There are products available to address this issue, such as "digital shredder" software, which erases data from the machine after each use.

- **Establish a corporate "neighborhood watch" program**. Set up a reporting structure that is able to detect irregularities and prevent social engineering.

- **Check the backgrounds of all employees who handle sensitive data**.

Alcatel·Lucent

PEOPLE (continued)

- Make sure the passwords for systems administrators have the strongest level of authentication and are given to the smallest potential audience.

  • **Require systems administrators to take two consecutive weeks of vacation annually**—similar to the vacation requirements for senior bank managers—so that fraudulent activities or other improprieties can surface while they are gone.

  • **Develop a policy-setting "security council"** that has an executive sponsor from each major department, such as human resources, finance, IT, and marketing.

  • **Integrate IT procedures and HR procedures** so that system access is tied to employee (and consultant) hiring and departures.

Alcatel·Lucent *(A)*

BEST PRACTICES -- PROCESS

• **Establish a reliable system for assigning access to company data**. Make sure the system can disable such access immediately if a major layoff occurs.

• **Determine**, based on job function, seniority and other roles, **who needs to have access to which company resources and why**.

• **Require employees to sign a nondisclosure contract** on their date of hire so they know what type of information is considered proprietary and what the consequences will be if they share it without authorization.

• **Keep an inventory of your IT assets**. Know the type and version of every operating system and application you use, as well as the number of computers and networking devices you have and all of the firewall types and rules.

• **Conduct security audits on all systems every 24 hours** to ensure that the systems are secured and have not regressed or been rendered vulnerable.

• **Make the ability to support your company's information access policy one of the criteria for buying new software or systems**.

• <u>Evaluate the security of your business partners and vendors</u>.

Alcatel·Lucent

BEST PRACTICES -- TECHNOLOGY

• **Identify dormant IDs or orphaned accounts**. Install or create a system for actively checking for and deleting out-of-date IDs and accounts as well as inactive users. (Make sure for employees & Contractors)

• **Have an automated system for resetting passwords** on a regular basis.

• **Make sure that the accounts belonging to laid-off employees are not simply deleted.** Instead, incorporate a suspend feature in your provisioning process that prevents outside access but enables the IT department to search for key data in the account.

• **Convert physical access-control devices from electronic systems to network enabled devices so that physical access events can be correlated with network events and file-access attempts.** For example, integrate your building-access card reader with your IT network so that an event like a person entering a building late at night can be correlated with any cyber security violations that take place around the same time.

Alcatel·Lucent *(A)*

TECHNOLOGY (continued)

- Deep Packet Inspection

- Encryption Technologies

- Access Monitoring

- IT Activities Logging

- Content Filtering

- Data Leakage Detection & Prevention

- Perform Vulnerability Tests

   on inside network perimeters

Alcatel·Lucent

PRACTICES THAT WORK FOR OTHER CORPORATIONS

1: *Institute periodic enterprise-wide risk assessments.*

2: *Institute periodic security awareness training for all employees*

3: *Enforce separation of duties and least privilege*

4: Implement strict password and account-management policies and practices.

5: *Log, monitor, and audit employee online actions*

6: *Use extra caution with system administrators and privileged users*

Alcatel·Lucent

BEST PRACTICES THAT WORK (continued)

7: *Actively defend against malicious code*

8: *Use layered defense against remote attacks*

9: *Monitor and respond to suspicious or disruptive behavior*

10: *Deactivate computer access ASAP following termination*

11: *Collect and save data for use in investigations*

12: *Implement secure backup and recovery processes*

13: *Clearly document insider threat controls*

Alcatel·Lucent

QUESTIONS ???

Alcatel·Lucent

Dr. Jim Kennedy

Principal Consultant & BCDR/Security Practice Lead

NCE, MRP, MBCI, CBRM, CHS-IV, Security+

jtkennedy@alcatel-lucent.com

Alcatel·Lucent