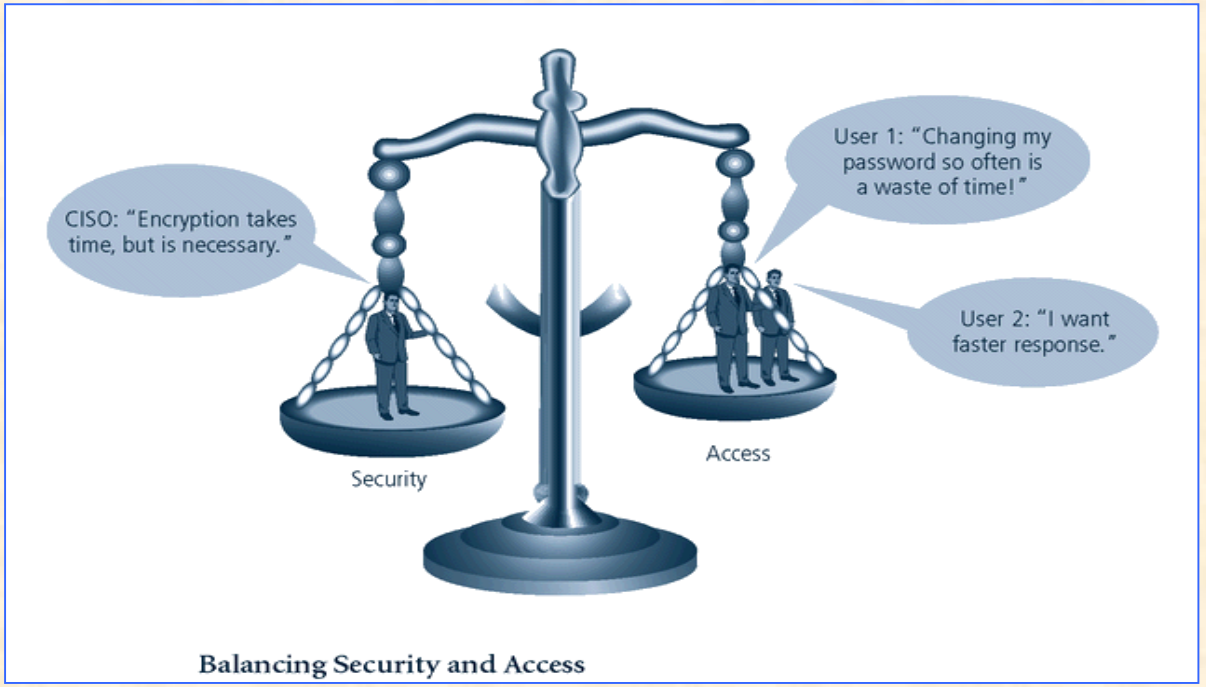
EE4758/IM3003 COMPUTER/INFORMATION SECURITY
TUTORIAL NO. 2

1. **Describe various types of security threats and explain why despite huge advances in technology and encryption techniques it is not possible to provide 100% security for a computer connected to an internet.**

- **Various Types of attacks**
- **Various Types of attackers**
  - **Criminal Attacks**
    - Basis is in financial gain.
      - Includes fraud, destruction and theft (personal, brand, identity)
  - **Privacy Violations**
    - Private/personal information acquired by organizations not authorized.
      - Includes surveillance, databases, traffic analysis

- **Publicity Attacks**
  - Attacker wants to get their name(s) in the papers
  - Can affect ANY system, not just related to profit centers
  - Denial of service.
- **Legal Attack**
  - Setup situation to use discovery process to gather information.

- Impossible to obtain perfect security
- Security should be a balance between protection and availability



Balancing Security and Access

2. What are the three characteristics of Internet that make online attacks easy to launch and difficult to detect despite the improved security technology.

1) Automation

- Speed of computers and networks makes minimal rate of return attacks possible.
- Data mining is easy and getting easier, affecting privacy

2) Action at a Distance

- Attackers can be far away from their prey and still do damage.
- Interstate/International differences in laws can affect prosecution

3) Electronic techniques easily transferable/duplicated

- Counterfeiting e-money
- Attack tools can be created by single person
- Easily modified per situation

3. Trace the history of computer security from 1960 to modern times?

☐ The 1960s

➔Students at the Massachusetts Institute of Technology (MIT) form the Tech Model Railroad Club (TMRC) begin exploring and programming the school's PDP-1 mainframe computer system. The group eventually coined the term "hacker" in the context it is known today.

➔Ken Thompson develops the UNIX operating system, widely hailed as the most "hacker-friendly" OS because of its accessible developer tools and compilers, and its supportive user community.

☐ The 1970s

➔Bolt, Beranek, and Newman, develop the Telnet protocol, a public extension of the ARPANet. This opens doors for the public use of data networks which were once restricted to government and academic researchers. Telnet, though, is also arguably the most insecure protocol for public networks, according to several security researchers and thus opened the doors for security attacks.

The 1980s

- IBM develops and markets PCs based on the Intel 8086 microprocessor thus aiding in the proliferation of such hardware in the homes and offices of malicious users.
- The Legion of Doom and the Chaos Computer Club are two pioneering cracker groups that begin exploiting vulnerabilities in computers and electronic data networks
- Courts convict Robert Morris, a graduate student, for unleashing the Morris Worm to over 6,000 vulnerable computers connected to the Internet.
- The next most prominent case ruled under this act was Herbert Zinn, a high-school dropout who cracked and misused systems belonging to AT&T and the DoD.

The 1990s

- Linus Torvalds develops the Linux. Because of its roots in UNIX, Linux is most popular among hackers and administrators who found it quite useful for building secure alternative.
- Vladimir Levin and accomplices illegally transfer US$10 Million in funds to several accounts by cracking into the CitiBank central database. Levin is arrested by Interpol and almost all of the money is recovered.

The 1990s

- Possibly the most heralded of all crackers is Kevin Mitnick, who hacked into several corporate systems, stealing everything from personal information of celebrities to over 20,000 credit card numbers and source code for proprietary software. He is arrested and convicted of wire fraud charges and serves 5 years in prison.
- Kevin Poulsen and an unknown accomplice rig radio station phone systems to win cars and cash prizes. He is convicted for computer and wire fraud and is sentenced to 5 years in prison.
- The stories of cracking and phreaking become legend, and several prospective crackers convene at the annual DefCon convention to celebrate cracking and exchange ideas between peers.
- A 19-year-old Israeli student is arrested and convicted for coordinating numerous break-ins to US government systems during the Persian-Gulf conflict. Military officials call it "the most organized and systematic attack" on government systems in US history.
- British communications satellites are taken over and ransomed by unknown offenders. The British government eventually seizes control of the satellites.

The 2000s

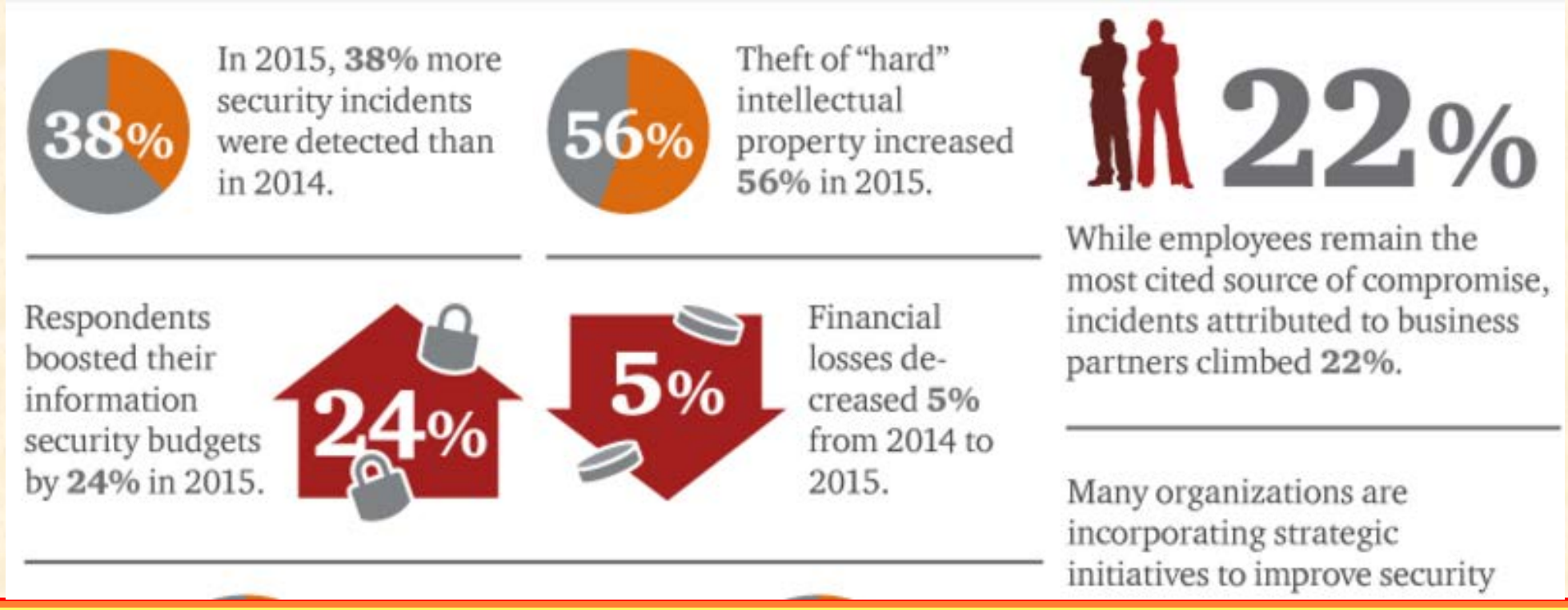
- In February of 2000, a Distributed Denial of Service (DDoS) attack rendered yahoo.com, cnn.com, amazon.com, fbi.gov, and several other sites completely unreachable to normal users.
- The worldwide economic impact of the three most dangerous Internet Viruses from 2001 -2003 was estimated at US$13.2 Billions.
- Estonia suffers massive denial-of-service attack.
- Conficker worm has infiltrated billions of PCs worldwide including many government-level top-security computer networks.
- The Stuxnet worm is found by VirusBlokAda. Its payload targeted just one specific model and type of **SCADA** systems. It slowly became clear that it was a cyber attack on Iran's nuclear facilities.
- An "external intrusion" sends the PlayStation Network offline, and compromises personally identifying information (possibly including credit card details) of its 77 million accounts, in what is claimed to be one of the five largest data breaches ever.
- The U.S Senate computers is hacked by hacker group Lulz Security. World bank, IMF and other high profile sites are also attacked.
- 6.5 millions LinkedIn members password stolen and published (2012).

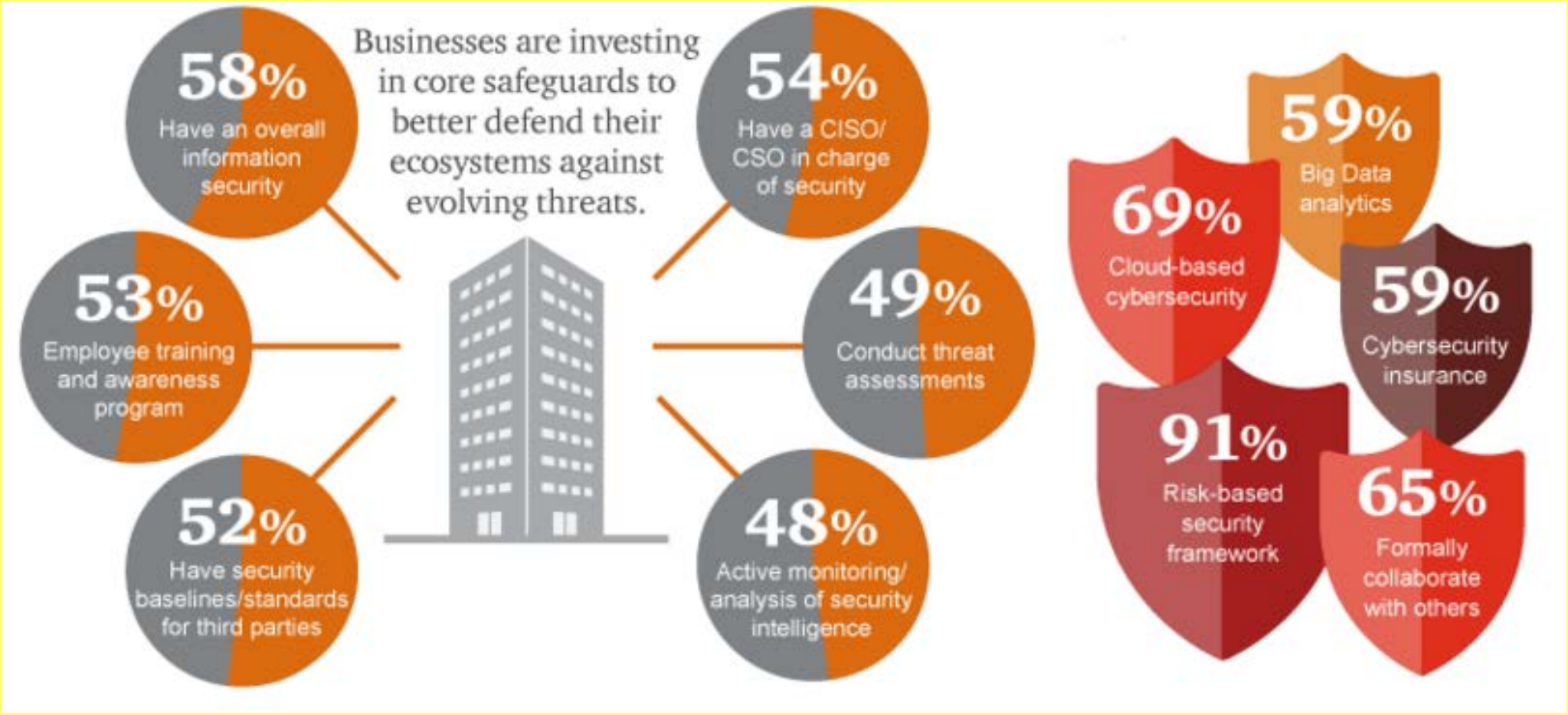
The 2000s

- In 2013, Facebook and Twitter accounts were compromised
- April 2013, LivingSocial: 50 Million Accounts Attacked
- October 2013, 38 Million Adobe Accounts were hacked
- May 2014, 233 million Ebay usernames, passwords, phone numbers and physical addresses were compromised.
- August 2014, 1.2 Billion passwords and 500 million email addresses from were stolen.
- October, 2014, J.P. Morgan Chase compromised information about 76 million households.
- Other famous data breaches in 2014 include:
  - ➔Sony data breach (The Interview)
  - ➔ iCloud hack (Celebrities were most affected)

The 2000s

- Estimated global cost of cyber attacks in 2015
  - $400 billion
- Projected global coast of cyber security in 2019
  - $2.1 trillion
- Source: http://expandedramblings.com/index.php/cybersecurity-statistics/




Businesses are investing in core safeguards to better defend their ecosystems against evolving threats.
58%
Have an overall information security
54%
Have a CISO/ CSO in charge of security
53%
Employee training and awareness program
49%
Conduct threat assessments
52%
Have security baselines/standards for third parties
48%
Active monitoring/ analysis of security intelligence
59%
Big Data analytics
69%
Cloud-based cybersecurity
59%
Cybersecurity insurance
91%
Risk-based security framework
65%
Formally collaborate with others

4. What type of security was dominant in the early years of computing?

- In the early years of computing when security was addressed at all, it dealt only with the physical security of the computers themselves and not the data or connections between the computers.
- This led to circumstances where most information being stored on computers was vulnerable since information security was often left out of the design phase of most systems.

5. Why is data the most important asset an organization possesses? What other assets in the organization require protection?

- Data is important in the organization because without it an organization will lose its record of transactions and/or its ability to deliver value to its customers.
- Since any business, educational institution, or government agency that functions within the modern social context of connected and responsive service relies on information systems to support these services, protecting data in motion and data at rest are both critical.
- Other assets that require protection include the ability of the organization to function, the safe operation of applications, and technology assets.

6. How can the practice of information security be described as both an art and a science? How does security as a social science influence its practice?

- The practice of information security is a never-ending process. An effective information security practice must be considered as a tripod that relates to three important aspects (science, art, and social science):
- First, information security is a science because it requires various kinds of tools and technologies used for technical purposes.
- Second, information security is also an art because there are no clear-cut rules on how to install various security mechanisms.
- Third, and most importantly, information security must be looked at as a social science mainly because social science deals with people, and information security is primarily a people issue, not a technology issue.
- Through the eye of a social scientist, an organization can greatly benefit from the Security Education, Training, and Awareness program (SETA), which can help employees (1) understand how to perform their jobs more securely, (2) be fully aware of the security issues within the organization, and (3) be accountable for their actions.
- Therefore, information security must be viewed as having all three natures, with the most emphasis on the social science perspective. After all, people are the ones who make the other five components of information assets (software, hardware, data, procedures and networks) possible.

7. Who decides how and when data in an organization will be used and or controlled? Who is responsible for seeing these wishes are carried out?

- The three types of data ownership and their respective responsibilities are:
- **DATA OWNERS:** Those responsible for the security and use of a particular set of information. They are usually members of senior management and could be CIOs. The data owners work with subordinate managers to oversee the day-to-day administration of the data.
- **DATA CUSTODIANS:** Working directly with data owners, data custodians are responsible for the storage, maintenance, and protection of the information. Depending on the size of the organization, this may be a dedicated position, such as the CISO, or it may be an additional responsibility of a systems administrator or other technology manager. The duties of a data custodian often include overseeing data storage and backups, implementing the specific procedures and policies laid out in the security policies and plans, and reporting to the data owner.
- **DATA USERS:** End users who work with the information to perform their daily jobs supporting the mission of the organization. Everyone in the organization is responsible for the security of data, so data users are included here as individuals with an information security role.

QUIZ

A. Which of the following is generally viewed as the first internet worm to have caused significant damage and to have “brought the internet down”?

I. Melissa

II. The “Love Bug”

III. The Morris Worm

IV. Code Red

- In 1988, the Morris worm was the first such program to cause significant damage to the Internet and basically prevented numerous users from being able to access the Internet.

B. Which of the following individuals convicted of various computer crimes was known for his ability to conduct successful social engineering attacks?

I. Kevin Mitnick

II. Vladamir Levin

III. Tmothy Lloyd

IV. David Smith

- Kevin Mitnick is one of the most infamous of computer criminals and was known for his ability to perform social engineering attacks. He at one point testified before Congress about how easy it was to obtain information from individuals by using social engineering techniques.

C. Which of the following virus/worm was credited with reaching global proportion in less than ten minutes

I. Code red

II. The Morris Worm

III. Mellissa

IV. Slammer

❖The Slammer worm has been the fastest propagating worm, doubling the number of infected systems every 8.5 seconds.

D. ---------- is the fabrication of information that is purported to be from someone who is not actually the author.

❖ Masquerading