Key Concepts in Cyber Security Part 1 of 2

Table of Contents

Governance

**001 Chris Evans: Okay let's talk about governance.

Overview

Key Concepts and Issues in Cyber Security

Cyber Security's Role in an Organization's Culture, Vision, and Mission

Cyber Security Governance

Federal Guidelines

Impact and Limitations of Laws Relating to Cyber Security

**002 In this section we're going to talk-- we're going to start with an overview of cyber security and introduce some terms and concepts that you'll see throughout the discussion here.

We're going to talk about cyber security's role in an organization. This really gets to the heart of what governance is and what it means to have a governance structure in place.

We'll finish up with some of the federal guidelines; and then some of the cyber security related laws that you'll probably encounter as you go through your cyber security duties.

Cyberspace

The electronic medium of computer networks, in which online communication takes place [Free Dictionary *"Cyberspace Defined"*]

Composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work

- Thus, the healthy functioning of cyberspace is essential to our economy and our national security. [The National Strategy to Secure Cyberspace, 2003]

**004 So it wouldn't be a good discussion about cyber security if we didn't start with a definition of what cyberspace is and what it means. So I will ask you: Short of reading what's on the slide, what is it that cyberspace means to you? If somebody said: "Tell me what cyberspace is," what would you say? Chances are anything you say is correct. However--

Student: I guess it's the online world, so to speak, you know, where you're doing transactions or getting information, reading email, checking pictures. There's- of course there's like real things to do that draw physicists and governments.

Chris Evans: All right. So the online world.

Student: The online world.

Chris Evans: eCommerce.

Student: Right.

Chris Evans: Business to business stuff.

Student: Social interaction.

Chris Evans: Social interaction. Yes, the less important things as opposed to-- right yes.

What does cyberspace mean to you?

Student: Virtualization.

Chris Evans: Virtualization.

Student: Yes.

Chris Evans: That's an emerging component of cyberspace I'd say. What else?

Student: Technology.

Chris Evans: Technology. Okay. There's technology; there's information; there's the processes people use within the technology or between the technology and the information.

Really cyberspace is everything that's connected to the internet: intranets within companies, computers, routers, wireless-- you name it, it's pretty much all within this global term called cyberspace.

So if it's this bucket called cyberspace, what do you put in it? It's everything that you just mentioned: the routers, the firewalls, the information itself; you know, the people that interact with those systems. Because believe it or not, you're a part of cyberspace; not that you have, you know, silicon chips in your head or anything like that but you are a part of cyberspace.

We'll talk about-- or you'll see that as part of threat discussions when you're talking about cyber security threats. What's the number one weakness in a computer system or in cyberspace?

Student: People.

Student: People.

Chris Evans: It's you; not you but you-- you as the- as a person.

Student: I know it.

Chris Evans: So generally take the conglomerate of all those things-- again, the computers, the servers, the routers, critical infrastructure pieces, businesses, enterprises-- put that all into a bucket and that's what really cyberspace is. It's a whole bunch of stuff.

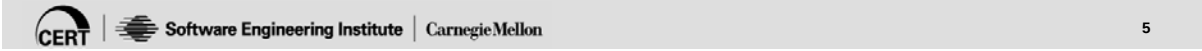
It's not a very easy definition.
So what do we mean by cyber security now?

Cyber Security -1

For the purposes of this course, we will use cyber security and information security interchangeably.

Defined as

> Protecting the confidentiality, availability, or integrity of information or information systems



**005 We're talking about securing all the stuff that we put into that cyberspace bucket. How do we secure those computers, routers, critical infrastructure? You as the end-user, how do we protect all of that?

And you'll see this discussed frequently: Confidentiality, Availability and Integrity. What are those three terms put together called? It's the CIA Triad. You'll hear this all the time within cyber security world. They talk about the CIA Triad. And it's not the intelligence agency pieces; it's this concept of confidentiality, integrity and availability.

So cyber security really is taking care of and addressing confidentiality, integrity and availability of the systems and the pieces and the people that are in cyberspace.

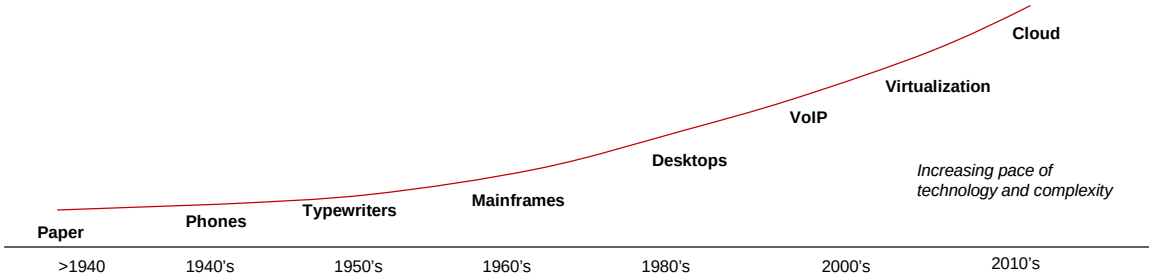
Cyber Security -2

Cyber Security -2

Information is an indispensable component of virtually all organizations and their ability to conduct business.

Information Security (IS) is becoming an increasingly critical program.

- It has become an integral part of enterprise management.
  - Affects an organization's leadership, structure, and processes
  - Now a responsibility of executive management and the board of directors



CERT | Software Engineering Institute | Carnegie Mellon 6

**006 When you look at cyber security, there's generally two aspects to it. There is the hardware piece that everyone equates: Oh I've got to secure my servers; I've got to protect, you know, the routers. So there's the hardware piece to this.

There's another aspect to it: the information piece that sometimes gets forgotten about when you're talking about cyber security.

So it's about protecting the systems; and it's also about protecting the information that resides on those systems. So you have this concept of information security really as kind of a separate component from cyber security. But what we're going to do throughout this class is we're going to call them one and the same. Because really when you're talking about cyber security, I think you have to address both the hardware piece and the information piece.

Why is it so important? Why is there all this effort and time and resources spent on cyber security; information security, information protection, information assurance? You'll hear all these different terms. Why is it so important? Any ideas?

Student: Well the critical information is about you and your personal information, the information about intellectual property.

Chris Evans: It's become-- I think that's it-- it's become so ingrained in our lives and within businesses and within governments that the idea of information security or cyber security, it really is now a critical function. Because how would you do your job without the computer system on your desk? I know World War 2, we used to fight wars without computers. How do we do that today?

Chris Evans: Okay, so we had the big banks in the--

Student: Big banks, yes.

Chris Evans: In the wall, in the closed rooms. And so but how would we do that today without the laptop, without the cell phone, without the satellite radio? I have no doubt the military's very resilient. We could do it. But I think it would be a challenge.

So because of this it's become an integral part of how we do business. It affects every single organization out there; every government, every business that's out there. And cyber security really has become a responsibility of executive management. Why is that? Because of the importance of information security now.

So whereas before executive management was like: "I'm running the business. My role as the CEO or the board of directors is to make sure that this business functions and we're making products and services" and that sort of thing. But now it's also: "I can't ignore technology."

Because you look, you know, along this little graph here, you can see the evolution of technology really has taken off; certainly within the last 30 years but even more so in the last 10 where you've got entirely new concepts out there--things that businesses and enterprises are relying heavily on, like Voice over IP or virtualization or cloud technology--businesses are relying more and more on this.

Where if you were to take this away, businesses would break; organizations, their business model would break. They wouldn't be able to do the things that they want to do or have to do.

And so because of this development and this increasing reliance on the pieces or the components within cyberspace, cyber security now has that corresponding critical function. You see more and more businesses, and more and more organizations, are taking that to heart. And that's why you see executive management like CIOs or Chief Information Security Officers now getting involved in this.

Cyber Security Requirements

**007 Cyber Security Requirements. How do you know what type of cyber security you need? How do you know how much you need? Any guesses?

Student: It depends.

Chris Evans: It depends. Okay, so that's my favorite answer. Because pretty much with anything related to cyber security, yes it all depends. But what does it depend on? Well I think it depends on your business: who you are; what you do.

Student: What you're trying to protect.

Chris Evans: What you're trying to protect; yes, the information that you're trying to protect or the systems you're trying to protect.

And it also depends on how much money, time and resources you can throw at it. Because chances are you probably are not one of the, you know, .001% of the businesses that have unlimited cash and can throw money at the problem to make it go away. So for the rest of us living in the real world, that's a resource constrained environment. Right? We can't do everything that we want to do, when we want to do it.

And so how much security do we need? Well we need enough to protect our systems and our information and the things we think are important to us; within reason. So as much security as I can afford-- meaning cost, time, manpower-- is probably what I should do for cyber security.

How do you understand, how do you know what pieces of security you actually want? Well a lot of this will come from business policy. And what we mean by business policy is executive management within your organization is going to say:

"These are the things that are important to us as an organization, or as a business. These are the things we need to protect; and to what degree we need to protect it."

So your areas of concern or the things that you want to devote cyber security to come from those policies. Based on that, you can derive your own requirements for: "Here's what I need to protect and how I'm going to do it." And then take the next step of: How am I going to afford it?

And if I have this grand plan for cyber security, but I can only afford this much of it because I've got limited manpower or limited dollars to spend on the program, what is most important to me? Do I protect, you know, Joe's email box or do I protect the Exchange Server? Where do I put those resources to?

Your executive management, your policies and your own interviews or your own discussions about what's important to the business will help you determine what type of cyber security pieces you put in place.

The other things I think you have to look at here are legal and regulatory requirements or concerns. Because the federal government--or if you operate in Europe EU-- will have different laws and regulations that you have to conform to. And so it might be grand to say that: "Okay well I'm going to spend this amount of money on cyber security, and that's all I'm going to do." But then the federal government can come down and say: "Okay, well you need HIPAA, you need FISMA, you need X, Y Z; you need to be

compliant with all of these laws and regulations." And so you need to account for that within your own cyber security requirements.

And we kind of already talked about risk analysis already. But it's this idea of how much security do you need? Well what are my risks? What are the impacts to my business? What do I actually need to protect? Based on that-- and we'll have a more detailed discussion on this-- but based on a risk analysis I can come up with: Here's what I actually need to do for cyber security. And that's a more informed decision based on impact to the business and real no-kidding risk that will help to inform what you actually need to do for cyber security.

Protection of Information Resources

"An organization's information and other intangible assets account for more than 80% of its market value."

- Study from The Brookings Institute

Some organizations are inherently information based.

As a governance function, protection of information resources has become a board-level activity.

- Computer crime, theft, hacking and vandalism are on the rise.
- There is an increasing demand for compliance and higher levels of accountability to new/existing laws and regulations.

CERT | Software Engineering Institute | Carnegie Mellon 8

**008 Protecting Information Resources. There's a great statistic here about, you know, information and other intangible assets account for an- account for 80% of an organization's market value or businesses' market value.

What this is really telling you is that there's a premium placed on information: intellectual property, the files and the information that you create, your data systems.

If you are in like an email marketing company, what is your primary driver for that email marketing company? Your customer database-- right?-- where you're

tracking names and email addresses. If that system didn't exist, you wouldn't exist as a business.

So what we see is a lot of organizations are very dependent on information systems and information. And in fact some organizations are entirely information dependent; meaning if that information goes away, they don't exist as a business, or their reason for being doesn't exist.

So from a governance perspective, really the protection of this information really becomes a critical- a critically important piece. And so you'll see board level-- you know, board of directors-- or CEO-- the C-suite level of management-- now getting involved to protect this sort of stuff.

Why are they starting to get involved? Well it's two things. One, it's the rise of information and the importance of information to a business. And it's also this rise of computer crime: hacking, computer theft, fraud and that sort of stuff.

You put those two together-- you have increasing importance of information, increasing rise in cyber crime-- and it means that it really becomes a-- it's really an important thing for businesses to address.

Information Security vs Information Technology Security

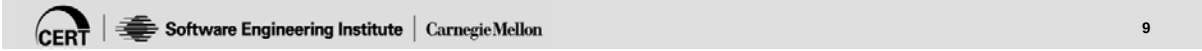
IT security is a component of Information Security.

Information Security

- Encompasses ALL aspects of information – content, meaning, knowledge
- Includes all aspects of risks, benefits, and processes involving information
- Governed by Executive Management

Information Technology Security

- Focuses on the security of information within the boundaries of the technological domain
- Governed at the Chief Information Officer (CIO) level



**009 Information Security versus Information Technology Security. So you'll probably hear the terms: Info security and IT security. What's the difference between the two?

Well if information security is the broad category of how do you protect all the information-- and what we mean by all the information is the content, the meaning, the knowledge itself; the value of the information is what you're protecting with information security.

IT security then is focusing on the information within those systems or within the technological system itself: what's residing on the server; what's in the router configuration or whatever have you.

And so you see different levels here. Again, information security is a very broad level program. IT security is more specific. And so because information security is a broad level program, you see that being managed by executive management: C-suite, board of directors.

Whereas usually IT security falls under the purview of either the chief information officer, usually. Sometimes it falls within the chief technology office or even the chief information security officer.

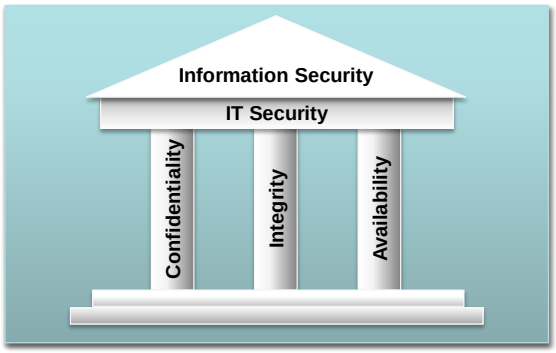
The CIA Triad

The CIA Triad

Confidentiality – Ensuring information is only available to those authorized to have access to the information

Integrity – Wholeness and completeness of the information without any alteration except by authorized sources

Availability – The ability to use the information or resource when it is needed



**010 We already talked a little bit about the CIA Triad. But here it is in its shining glory.

What do we mean by confidentiality? You're protecting information from disclosure. Right? You have a certain piece of information. You don't want other people to see it who aren't authorized to see it. That's confidentially.

Integrity-- what is that? We're trying to protect the integrity of data; meaning we don't want it to be changed or altered without appropriate permissions; or we want the right people to be able to change that information. That's protecting the integrity of data.

And availability is protecting the availability of information; meaning: I want that system to be available when I need it, when I need to use it; so that when I log into a system that information's there and I can have access to it.

And so really you see these as, you know, these pillars within IT security and within information security. So again, at the very top level you've got information security. A subset of that is going to be IT security; and then within IT security and information security you're focusing on really protection of three things: confidentiality, integrity and availability.

Operational Balance -1

Businesses' operations have become more complex, computing has evolved to become more sophisticated to support these operations

- Online applications for commercial use
- Data storage
- Virtualization
- Cloud computing
- IP-based communication (voice and video)
- Data transfers
- Email

**011 So there's this concept of operational balance; meaning businesses are more complex, there's more focus on data and technology. So you have businesses that are now doing things like using online applications, data storage, virtualization, Voice over IP, email systems.

How complicated is email? What actually goes into sending and receiving emails? Quite a bit actually; if you look at the bits and bytes that happen there.

Let's start at let's say John's desktop. Right? What do you have there? There's a computer system. Okay, got a computer system. In order to send email

he needs a email client, or perhaps a web browser. But let's say he needs Outlook or something like that.

So he's now got an application. What does he actually communicate with? Well he's talking to an email server. Right? What does that email server communicate with? Other email servers. Oh by the way, it has to go through routers and switches and everything to get to- you know, interact and interconnect with each other.

Who's on the distant end? Who's receiving an email message? Okay, so they have a desktop and they have an email client as well.

So just for a very simple example of email, look at how many pieces and parts that have gone into actually being able to give you the ability to send and receive email. It's a big, long chain of systems, applications, servers; there's a whole bunch that goes into there.

Why did I choose this really silly example? Well consider email is one small part of what you interact with and do as a business. Combine all of this stuff and what do you have? You have a big problem is really what you have. You've got all of this stuff out there, and it's very complicated.

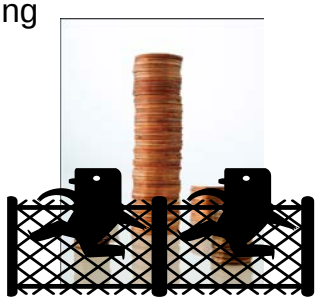
You need to do something about it.

Operational Balance -2

The security of these functions cannot override the ability to operate them

Risk analysis helps to identify security requirements based on operational needs, threats, and impact from those threats

- Database with no outside connectivity could be considered secure, but the operational effect of denying access to it makes the security pointless
- Cost-Benefit analysis can help you avoid “building a $10,000 fence around a stack of quarters”



**012 So if you focus on or over-focus on security of all those complex systems that we just showed on the previous slide, what can happen? Well you have to balance operations-- the ability to do email, Voice over IP, storing data on a file server-- with security.

If you have Draconian security-- meaning everything is locked down and people can't communicate-- what happens? You can't do your jobs. Right? And users will find a way to get around whatever security things you have put in place anyway; if it's too difficult. So now you're introducing additional problems here.

But the point behind this is that you can't override the function of things with security. So you can't come in and say: "Security, security, security" and expect things to work. Right? You have to balance the ability for me to do my job, as somebody sitting behind a computer, with the need for security.

So how do you get around this problem? How do you actually do this operational balancing? Well it really comes down to a risk analysis and the idea that you protect what's critical to you, based on the resources that you have, and don't break what you need to do your business.

So there's a careful balance again between operations and security. The best way to do that is with a risk analysis; make sure it's a risk-based approach.

So you might say-- as an example here-- you might say that you've got a database system-- right?-- and in order to protect it from being hacked into or taken advantage of you say, "Disconnect it from the internet."

Okay, well that's great security. But from an operations standpoint that might not be so good; because now you can't have connectivity to it, businesses can't talk to other businesses over this- with that database, and it makes-- the end result is you've defeated availability of the system. So you've become your own cyber risk, as it were, by implementing- over- implementing security.

There's a saying out there that you don't want to build a $10,000.00 fence around a stack of quarters. What do we mean by that? We're saying: Make security relevant and proportional.

So if this little widget cost $5.00, do I want to spend $20,000.00 protecting it? Probably not; unless this is like super-super-duper mission critical, the world will end if this thing falls on the floor, probably don't care, I'll just allocate $5.00 in my budget to replace this when Chris throws it across the room and it breaks. As opposed to putting in, you know, like-- you know, an engineered solution to prevent this from breaking when Chris throws it across the room.

Access Control

Effective access control ensures appropriate access to information and applications, and does not abuse it. **(C-I-A)**

Access control is about managing direct access to

- Information
- Computer applications
- Operating system facilities

Management issues, such as periodic reviews of user accounts, can apply as much to IT systems as to physical access control systems.

Confidentiality of information is best achieved by ensuring that people only have access to the information they actually need.

Ref: Information Security Standard ISO/IEC 27002; www.berr.gov.uk

**013 You'll hear this term 'access control'. What is access control? Access control is the idea that you are restricting access to systems, information, what have you, based on who are you, what role you have within the organization.

And it's about protecting, again, or ensuring, confidentiality, integrity and availability of systems. But you want to manage access to these systems, or this information, or even facilities-- so like let's say the server room-- you want to protect access to that. How do you do that? Well it's a broad category of things that all fall under access control.

So you have this idea that-- let's take an example from the physical world. Right? Everybody has keys to open doors or something like that. How do you make sure people have the right keys? And how do you make sure people have the keys that they're supposed to have; and only the keys that they're supposed to have? It's a management process. Right? Okay?

So this isn't a trick question. It's-- I know, I saw a bunch of blank stares. No, no it's not a trick question. It's a management process. Right? So I sign out a key to you; I know you have it. When you leave the company, I know to get the key back from you. It's a process. Right?

Well the same thing holds true for access control and information systems. When you join a company you get a set of permissions. It gives you access to this bunch of information or these systems. When you leave the company, what should happen is those permissions should be taken away. Or when you move someplace within the company those permissions need to be adjusted.

Where does this process break? Usually not in technological implementation; it's the management process of it. Right?

So when I changed jobs or changed roles, nobody came through and removed what I needed to do in my past job; they just gave me what I needed to do in my new job. So now instead of having access to this, I've got access to this much information or this many systems. Because they didn't go through and scrub the list of- the list of systems I needed access to.

So really it's the process that breaks here not the technical implementation of it. But by access control what you're really trying to do is ensure confidentially. Again, you're restricting access to information to who needs it; and only to people who need it.

Notices

Notices