Elevator Speeches for Business Leaders

Rebecca Herold, CIPP, CISSP, CISA, CISM, FLMI

Final Draft for November 2007 CSI Alert

Over the years I have had the great opportunity to speak with many business leaders in the CxO positions, along with many information security and privacy practitioners. I have found some of the topics and questions to be noticeably recurring. This month I want to discuss some of these frequently asked questions. Business leaders across the board want to know about these information security, privacy and compliance topics. Know how to answer them when your CEO, or other CxO, is in the elevator with you, or behind you in line at the cafeteria.

1. What are the personal risks that business executives face if they fail to implement effective security controls or do not comply with data protection regulations?

It is important for business leaders to first understand there are many laws and regulations requiring information security programs; some directly and some indirectly. These information security programs must be built based upon risk assessments related to safeguarding customer and personally identifiable information (PII) information, along with the systems where they are processed and stored.

In the U.S. the laws and regulations include, but are not limited to, the USA PATRIOT Act, the Sarbanes Oxley Act (SOX), the Gramm-Leach Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), the Federal Trade Commission Act (FTC Act), and the Fair and Accurate Credit Transactions Act (FACTA).

Many of the regulatory oversight agencies provide clarification for specifically what they are looking for with regard to compliance. For example, in the financial industry the FFIEC IT Examination Handbook, the FDIC IT Examination Workpaper, the OTC Consumer Regulations Handbook, the Federal Reserve Commercial Banking Handbook, the NCUA Regulatory Compliance Handbook, and the OCC Examination Booklet for Privacy of Consumer Financial Information all describe the importance and responsibilities of executive leaders to ensure security is in place.

In addition to the U.S. federal laws, there are at least 39 state level breach notice laws, hundreds of other state laws addressing data protection, and contractual obligations, such as PCI DSS and those contracts business partners have with your organization. Outside the U.S. there are over 100 country-level data protection laws.

Business leaders must work with the organization’s board of directors, or an appropriate committee of the board, to satisfy specific requirements designed to ensure that the institution’s information security program is developed, implemented, and maintained. The executives and board are ultimately, personally, responsible in many cases.

As just one example, under SOX the executive leaders of any publicly traded organization in the U.S. are personally liable for shortcomings in compliance requirements and face not only penalties but also jail time. The financial institution also faces not only penalties, but also bad publicity and lost customers.

The bottom line 30-second elevator speech for this topic that you could use follows:

> *You, as our organization's business leader, are ultimately responsible for ensuring we have a strong security program in place. If you don't, you personally could get substantial fines and penalties, even including jail time. You also subject our organization to significant fines and penalties, civil suits, diminished brand value, lost customers, and possibly the loss of our business.*

2. What approach should business leaders take to start an effective risk management program?

First and foremost, an organization needs to have strong support from executive leaders. Implementing a risk management program will involve personnel from throughout the organization, so it is important for executive leaders to communicate to all personnel that risk management is very important to the business, and that all personnel must be involved to be successful. Initiatives that involve the entire company will not be successful if the company leaders do not visibly support them; personnel will choose not to be involved if they believe business leaders do not care whether or not they are involved.

Second, you need to establish a good team to build the program that is headed by a strong and experienced leader. Many organizations that do not have someone in-house with risk management, information security and/or compliance experience benefit greatly by bringing in a consultant who has a large amount of experience doing this.

Third, don't try to reinvent the wheel; use well-established and proven risk management frameworks. Organizations benefit greatly from using, for example, COSO (Committee of Sponsoring Organizations of the Treadway Commission; a U.S. private-sector initiative, formed in 1985), COBIT (Control Objectives for Information and related Technology; a set of best practices for information technology management created by the Information Systems Audit and Control Association (ISACA), and the IT Governance Institute (ITGI) in 1992), and ISO 17799 (now called ISO 27002; an information security standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)) as the frameworks around which to build their information assurance and risk management programs.

Usually no single enterprise risk management framework is comprehensive enough to help you ensure your organization meets all of its compliance, governance, and risk management needs. Selectively combine standards by building around a central framework, such as COSO, and reinforcing it with one or more of the other risk assessment standards, such as COBIT and ISO 27002.

Fourth: Perform a risk assessment. Risk assessments are the foundation of any good security program, allowing an organization to truly understand the climate of their network and computer systems, along with revealing the risks involved with how the personnel handle the information.

The bottom line 30-second elevator speech for this topic that you could use follows:

> *Our risk management and information protection program needs to be improved. It will be more effective with the following four components:*
>
> 1. *Your strong and visible support for the program.*
> 2. *A good team representing the enterprise, with a strong and experienced leader.*
> 3. *A foundation built upon proven information control and technology frameworks.*
> 4. *Controls based upon our organization's own unique risks.*

3. What are some of the most common ways that information is leaked or compromised?

There are many ways in which sensitive information, such as personally identifiable information (PII) and top-secret business plans are leaked. Based upon reported incidents and multiple research studies, the top five common ways in which information is leaked and compromised seem to be the following, in no particular order:

- Via email. Many incidents have occurred when people send email containing sensitive information accidentally to the wrong people, when they forward email outside the company not realizing sensitive information is attached, and when email containing sensitive data is intercepted by unauthorized individuals.
- Through mobile computing and storage device theft and loss. Many privacy breaches have occurred when personnel have loaded PII and other sensitive information onto mobile computing devices, such as notebook computers and PDAs, and mobile storage devices, such as USB thumb drives, and then had those devices are lost or stolen. Most of the time the data on them is not encrypted.
- Not building security into applications and systems, resulting in data being inappropriately posted or accessed. When security is not considered from the very start of updating or building a new system or application, and when security is not thoroughly tested before launching it into production, the chances are high the data processed within the application or system will be compromised. Many incidents have recently occurred because of poor programming that allowed security vulnerabilities.
- The insider threat. Humans are the weakest link in the information security and privacy chain. Authorized individuals often make mistakes with PII, resulting in security incidents and privacy breaches. A significant amount of authorized personnel maliciously take, alter, copy, or delete information.
- Improper disposal of PII. Organizations that spend significant amounts of time and effort protecting the network perimeter often completely forget about securing information at the end of its lifecycle. However, significant security incidents and privacy breaches have occurred as a result of not removing data from hard drives when they are retired, by not shredding sensitive paper documents when they are thrown away, and by not deleting voice mail that is no longer needed.

The bottom line 30-second elevator speech for this topic that you could use follows:

> *We are vulnerable to having PII and sensitive data leaked, resulting in costly information security incidents and privacy breaches, largely due to the following:*
>
> - *Sensitive data included within or attached to email messages.*
> - *Mobil computing devices and storage devices that are lost or stolen.*
> - *Applications and systems that are built without properly addressing security controls.*
> - *Authorized persons making mistakes or purposefully doing malicious things.*
> - *Disposing of computers, storage media, and paper without first removing sensitive information.*
>
> *I need your support for the initiatives to address these vulnerabilities.*

4. What should we do to secure mobile data?

Mobile data, that which is sent through networks or is stored on devices that move, such as notebook computers, smart phones, CDs, and USB drives, can generally be secured by taking five actions:

- Establish executive -supported policies for the use of mobile computing and storage devices.
- Establish procedures to support those policies. Each department within the enterprise should create supporting procedures based upon how the areas send data through the network, and how they use data on mobile devices.
- Provide training to all personnel about how to secure mobile computing devices and storage devices. Provide targeted training to groups based upon how they send and store mobile data. For example, sales personnel and brokers will need to have training targeted to their habits, which will be different from how the e-commerce applications developers send sensitive data through networks.
- Provide ongoing awareness communications about how to secure mobile devices. Communicate often in many ways about the threats to mobile data.
- Do not allow PII and other sensitive information to be stored on mobile computing and storage devices. If this is not feasible, then implement strong encryption on those devices.

The bottom line 30-second elevator speech for this topic that you could use follows:

> *PII and other types of sensitive information that pass through networks and are stored on mobile computers and storage devices are highly susceptible to security incidents and privacy breaches. We need to protect this mobile data by:*
>
> - *Having business leaders, such as yourself, strongly support policies and procedures for protecting mobile data.*
> - *Encrypting mobile PII.*
> - *Providing training and ongoing awareness to personnel for how to safeguard mobile data.*
>
> *I need the support and resources to protect our mobile data.*

5. What should we do to keep personnel from making mistakes or doing malicious activities?

The very short answer is education, training and awareness! All organizations that handle any type of PII and/or sensitive information need to provide training and ongoing awareness communications to personnel about how to keep information safe while performing their job responsibilities. Humans are the weakest link in the information security chain; they must receive ongoing training and awareness for any information security program to be effective.

When creating your awareness communications and training curriculum you must first and foremost, know your business. You cannot creative an effective information protection education program without knowing your business. Your education program should be based upon the results of your risk assessment. Too many information security practitioners try to implement off-the-shelf information security training modules as is, or just copy information off the Internet to push out to their personnel to call training, without first knowing what their business is and what threats and vulnerabilities exist within the business. Information security education is not effective if it does not address your business' risks.

Another aspect of information security and privacy education is communicating directly and often with business unit leaders. This will help you to better understand how they perform their business, and will also provide an opportunity for them to have input to your information security program. When people have input to the program, they feel a sense of partial ownership and will be more likely to not only buy-in to your information security efforts, but also to actively support and promote your information security initiatives.

The bottom line 30-second elevator speech for this topic that you could use follows:

> *People will make costly mistakes if they do not receive information security training and ongoing awareness communications. Personnel who want to misuse their authorization to commit fraud, crime, and perform other malicious acts will be able to do so more easily if the workforce is not provided information security education and taught how to recognize the red flags of those around them. If you visibly and actively support our information security and privacy education efforts, we will have personnel who safeguard our business information better, and ultimately improve our business.*

Be Prepared For Your Elevator Pitch!

Of course you will need to tailor the answers to the previous questions to fit your own, unique business, organization's culture, and your personal relationship with the CxO you will be speaking to. When thinking about your elevator speech, you need to consider the following:

- Your relationship with your CxO should guide how direct you are with him or her. The speeches I provided are pretty straight-forward since I was used to speaking with my executives in that manner. However, it may be more effective for you to use more tact or "soft-selling" with your executives.

- Be sure that your elevator speech points out a risk area and/or problem and why the executive should be concerned. Do not to describe the details of your concern in 30 seconds.
- The goal of your CxO elevator speech is to develop a rapport with the executive and get his or her attention about information security and privacy. You want to pave the road to a more lengthy and detailed meeting in the near future on a topic that is important to the organization.
- The goal of your quick executive elevator chat is ***NOT*** to communicate everything you know about the topic to the CxO.
- Remember, your elevator speech is an awareness-raising opportunity, not a training session in and of itself.
- Don't be afraid to ask your CxO for his or her visible support! Don't assume that the CxO knows or understands that his or her support is essential for information security and privacy success.

These suggested elevator speeches can provide the basis upon which you can create your own elevator speeches and be prepared to take advantage of those often rare moments when you get the ear of your executive leaders. As an added bonus, you can also use these conversation starters during professional membership meetings and gatherings to establish networking opportunities with your professional peers.

Always keep in mind when you are speaking to your executive leaders that you are providing information security, privacy and compliance initiatives and management to ***SUPPORT THE BUSINESS***. Too many practitioners, and consultants for that matter, implement information security for information security's sake. Too many use what sounds like techno-babble when they speak with business leaders. Learn to talk your executives' talk to be more effective in your information security and privacy initiatives.

Rebecca Herold, CIPP, CISSP, CISM, CISA, FLMI is an information security, privacy and compliance consultant, writer and Norwich University MSIA adjunct professor. She just released the quarterly employee awareness tool, “Protecting Information” (Information Shield) and blogs daily at http://www.realtime-itompliance.com. She can be reached at rebeccaherold@rebeccaherold.com or http://www.privacyguidance.com.