WEST-CENTRAL AFRICA DIVISION

Business Professionals Convention

Grand Bassam 2017

The Role of the CFO in IT Governance

By Mabio Coelho

CISO of General Conference

The CFOs should also be concerned with Cyber Security because one little word called Liability. In organizations like ours, that generally don't have CSOs/CISOs, or when they have they are not really Officer of the corporation, the liability of breaches and incidents is the CFO's responsibility. In most jurisdictions, including here in Australia, CFOs can be personally liable.
The CFO has an important and ongoing role to play in risk assessment, incident management, and incident response planning—key components of any security strategy. Analyzing the feasibility and cost effectiveness of cyber insurance and security solutions also falls in the CFO's area of expertise and advisement.

On tomorrow's presentation we will talk more of some practical things you can do about it to protect the church and yourself against liability.

Security is an Governance Issue

"The rising tide of cybercrime and threats to critical information assets mandate that boards of directors and senior executives are fully engaged at the governance level to ensure the security and integrity of those resources."

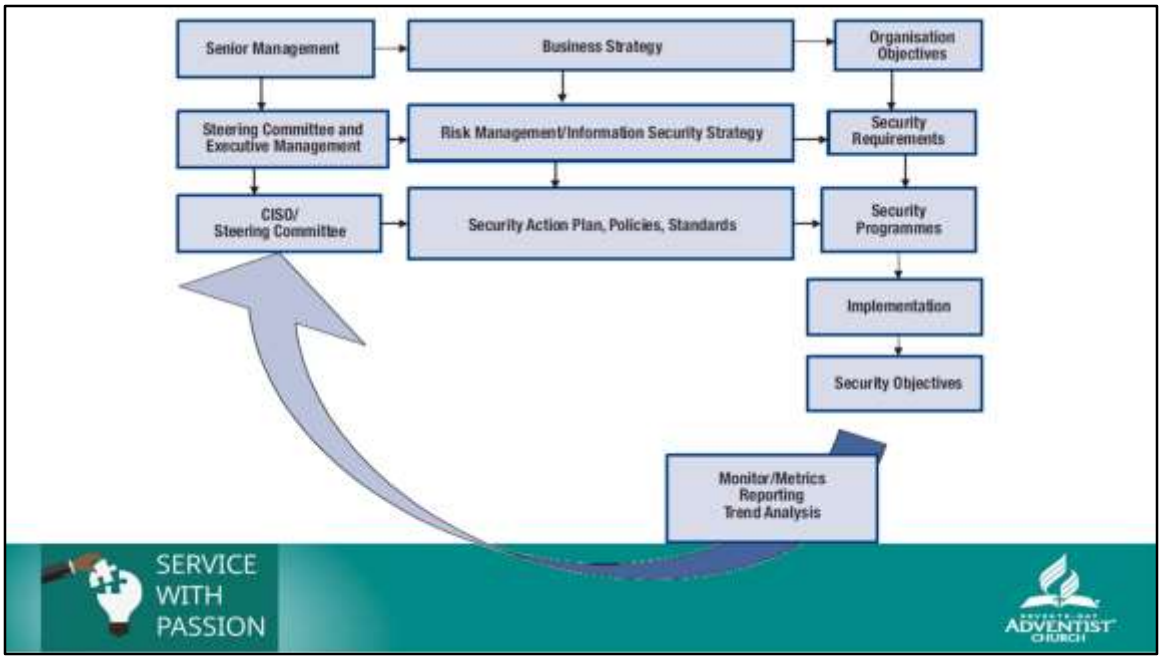
— SHIRLEY M. HUFSTEDLER, BOARD OF DIRECTORS
HARMAN INTERNATIONAL INDUSTRIES

By the way, The Chartered Institute of Management Accountants (CIMA) and the International Federation of Accountants (IFAC) also adopted this definition in 2004.

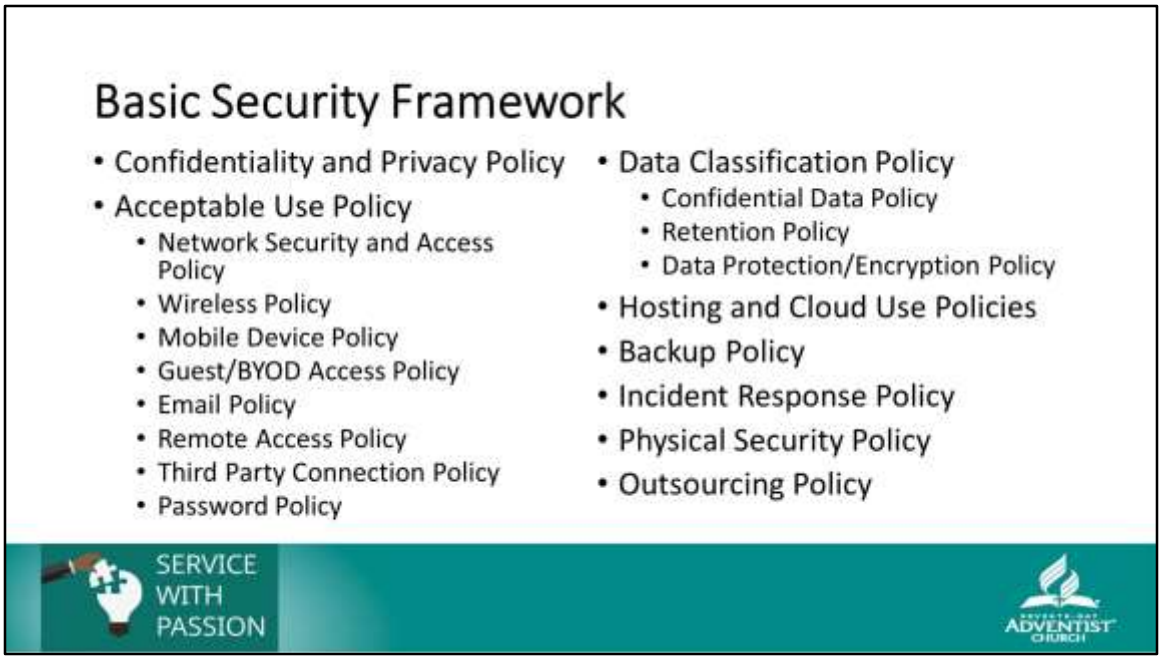
Note that is a executive responsibility to provide strategic direction to assure note only resources are used responsibly (and by responsibly it is meant not only in financial terms, but in terms of security and compliance.

Information security governance isn't about the technical aspects of IT security. It's about defining responsibility and accountability, and structuring policies to ensure that decisions are made in such a way that they help an organization achieve an accepted level of risk.


CONDUCT
LAW
PROCEDURE
RULES
GUIDE LINE
COMPLIANCE
CONSTRAINT
STANDARDS
Security ≠ Compliance
SERVICE WITH PASSION
To be secure you need to be Compliant!
ADVENTIST CHURCH



In order to work in our organization (or in any organization for that matter), is to follow a governance model that kind of look like this Conceptual Information Security Governance



Please check and become acquainted with the new set of IT and Security policies on the General Conference Working Policy book (BA72 family of policies). They will guide you and help you to implement that basic security framework and IT Governance models.

This is both necessary for compliance/audit purposes and to enable your organization to be insurable (for Cyber Liability Insurance).

Supporting Documents and Forms

- Policy Acknowledgement Form
- Security Incident Report
- Notice of Policy Noncompliance
- Account Setup Request
- Guest Access Request
- Request for Policy Exemption
- Risk Acceptance Form

With that model in mind, and also remembering that you, as the CFO without a independent CSO/CISO, are personably liable, what you should be aware of?

Cybercrime-related intelligence relating to emerging threats should be reviewed by the CFO on a regular basis to determine:

1 – How likely you are of being attacked and how probable this attack is to succeed?

2 – How information from your key users and applications (which might be targeted) can be used by criminals.

3 – Know what techniques the hacker may use on you and your critical systems

Some of you still not getting the point why security is important at the first place. Why bother with all that?

As the breach of financial wire services (like SWIFT) aptly demonstrates, attackers have become more organized, sophisticated, and dangerous. They are able to operate undetected for extended periods, intensifying the damage done to both reputations and bottom lines. Cybercriminals and hacktivists increasingly target brand reputation and the interdependencies amongst suppliers, customers and partners. CFOs can defend against these attacks by identifying and prioritizing the protection of their organization's most valuable data, assets, and relationships.

Before we go over some strategic initiative CFOs should and must get involved, I need to give you some insight how is the current state of cyber crime to help you understand why this is important enough to be part of your agenda.

What Cyber Crime use to be

SERVICE WITH PASSION

SEVENTH-DAY ADVENTIST CHURCH

On the past, hacking use to be an individual effort. Lone wolves on a basement, doing stuff for fun or profit.

Cyber Crime Today

SERVICE WITH PASSION

SEVENTH-DAY ADVENTIST CHURCH

Ciber crime today is a corporate business. There are many underground “companies”, with 8 hours/day, 5 days a week working schedules, target and goals, bonuses, employee vacation. Just like a normal business, but their main product is hacking tools and services.

Today you can buy from those enterprises attacks with different service levels (Gold, Silver, Bronze)

On the dark web you can even buy attacks with Money Back Guarantee.
You, pretty much as you do in amazon, you can rate your merchants, review.

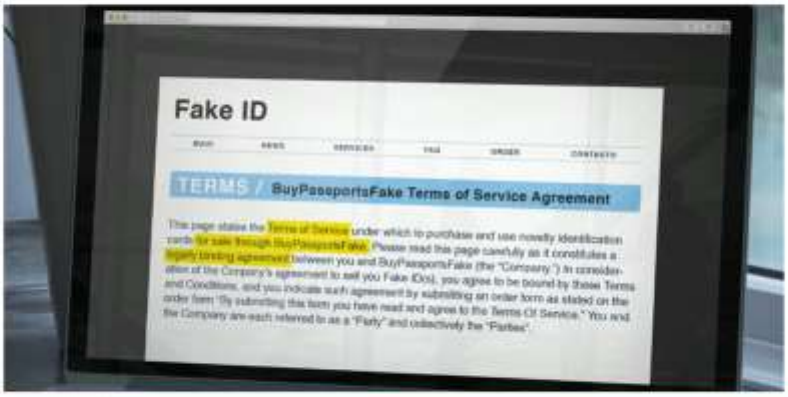
Example of a Malware store

SERVICE WITH PASSION

SEVENTH-DAY ADVENTIST CHURCH

They are even rated for customer service/support, efficiency and effectiveness.

Example of a Malware store



SERVICE WITH PASSION

SEVENTH-DAY ADVENTIST CHURCH

Note the terms of service: Legally binding agreements

1 – Provide Security Education

SERVICE WITH PASSION

Education is the first line of defense. Working with your Division IT to get access to the resources the General Conference is providing you.

Data Classification is the Keyword:
In response to the growing number of breaches, many companies have taken an overly cautious approach, deciding to strictly protect all of their data. However, not only does this come with a hefty price tag but, since resources are often limited, it could also mean overlooking some valuable assets.

According to a 2014 study from Saugatuck Technology, many finance departments tend to be more cautious when it comes to moving data from the "money" function – such as treasury, core accounting and revenue management data – to the cloud, but tend to be less concerned with managerial data such as expense management, planning and forecasting. Not all information is critical or confidential – in order to prioritize data protection needs, CFOs should work with their finance teams to evaluate which data is critical and rank it appropriately.

In today's digital world, cybersecurity is an issue that is top of mind for every company. Whether it's worrying about the malware threat from employees chasing Pokemon around the office, to large-scale breaches such as that seen with Wendy's earlier this year, executives face a greater challenge than ever in ensuring that data is protected in the enterprise.

Specially important to keep in mind if you don't have an CSO/CISO who is trained/qualified and is responsible for your security, which is the case of most of you here. There is no silver bullet! You have to follow the processes and, at minimum, new implement the policies suggested by the Working Policy.

4 – Sponsor a Incident Response Plan

SERVICE WITH PASSION

If you have a CSO/CISO or somebody responsible for security, give support and executive sponsorship in the preparation of a comprehensive Emergency/Incident response plan.

Focus on the controls for the “crown jewels” and what you would do in the event of an incident.
The team responsible for this should include senior management from the lines of businesses and administrative functions.

5 – Get periodic Security Reports

SERVICE WITH PASSION

Make time in your busy schedule to meet at least once a quarter with your CISO/CSO or Senior IT administration.

These reports should be from senior management and detail privacy and security risks, based not on project status but on specific risk indicators.

Nothing is bullet-proof. Not all risks can be mitigated.

We do our best to make sure our buildings will not burns. I have to say that all CFOs I worked with in my career, both in the church and outside, always made sure everything they build had all the safeguards to protect their investment on the building and the people in it. But I also have to mention that all, without exception, had an insurance policy in place. And I did not even had to ask.

As CFOs is you duty to have the same zeal by making sure you have a cyber liability policy in place for those fatalities that can mitigated. If you want to know more about that, let me know. You can also reach ARM and they will help you with that

Questions?

By Mabio Coelho (coelhom@gc.Adventist.org)

For purchase request write to: