Security Challenges and the Need for More Effective IT/Business Relationships – The Wrap

On February 18th 2016, the CIO Executive Council (CEC) hosted a webcast that explored the increasing impact security challenges have on both IT and business stakeholders, as well as how IT management, the Board, and others within an organization can effectively work with each other in optimizing an organization's security policies, posture, and capabilities. Taking part in the presentation were: ***Scott Angelo****, CIO K&L Gates;* ***Mike Plantinga****, CIO CIBC Mellon; and* ***Steve Ragan****, Senior Staff Writer, CSO Online.*

The following is a summary of key points made during the webcast, which can be viewed in its entirety by clicking here: Security Challenges and the Need for More Effective IT/Business Relationships.

Key Points from the Webcast:

- Security is always going to be a top spend, The Computer World Forecast for 2016 predicts that the greatest increase in spending will be in security technologies (50%), followed by cloud computing (48%).
- Companies are learning from their mistakes but criminals are clever and it's the little things, like hacking, that usually make organizations vulnerable. Sixty-four percent of the incidents that happened last year were the result of hacking.
- The top three security challenges for 2016:

    1. **Data Leakage** - strengthen what information is leaving the company, knowing what information is allowed to leave the company, and knowing how to balance these two;
    2. **Vendor Security** - know what the organization's vendors are doing, make sure that vendors have the same strength in policies, procedures and controls;
    3. **Readiness** - knowing how to prepare for a cyber-security event.

Tips on Preparing for a Cyber-Security Event:

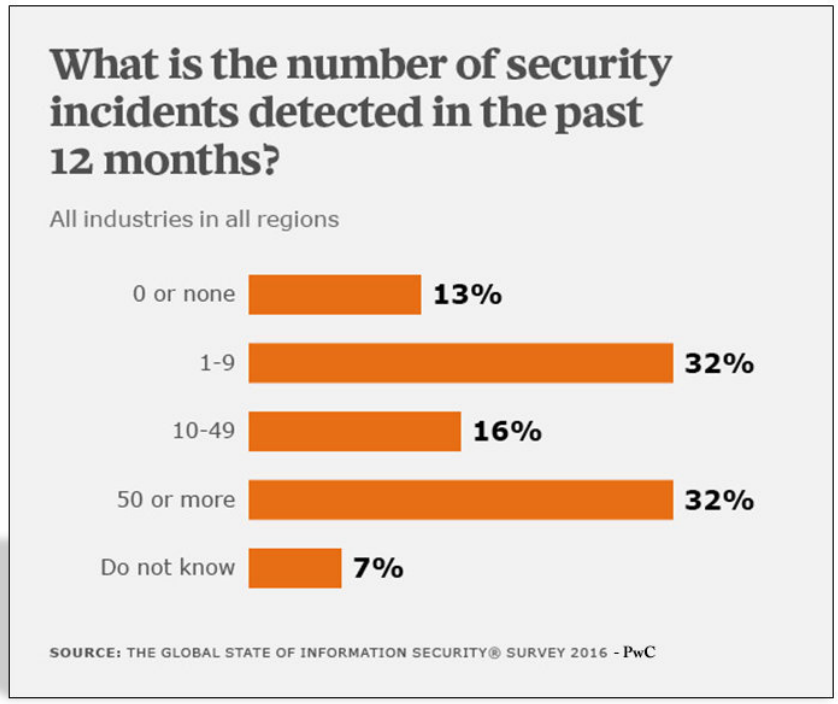
- Think about the communication strategy used once the problem is contained, and how the issue communicated to the public, regulators, clients, and employee base.

- Organizations should have a solid **threat model**: one that understands the hardware or data points that are on their network and how far their network extends beyond the server room. They should also understand asset management.

- There are three levels of prevention and detection:

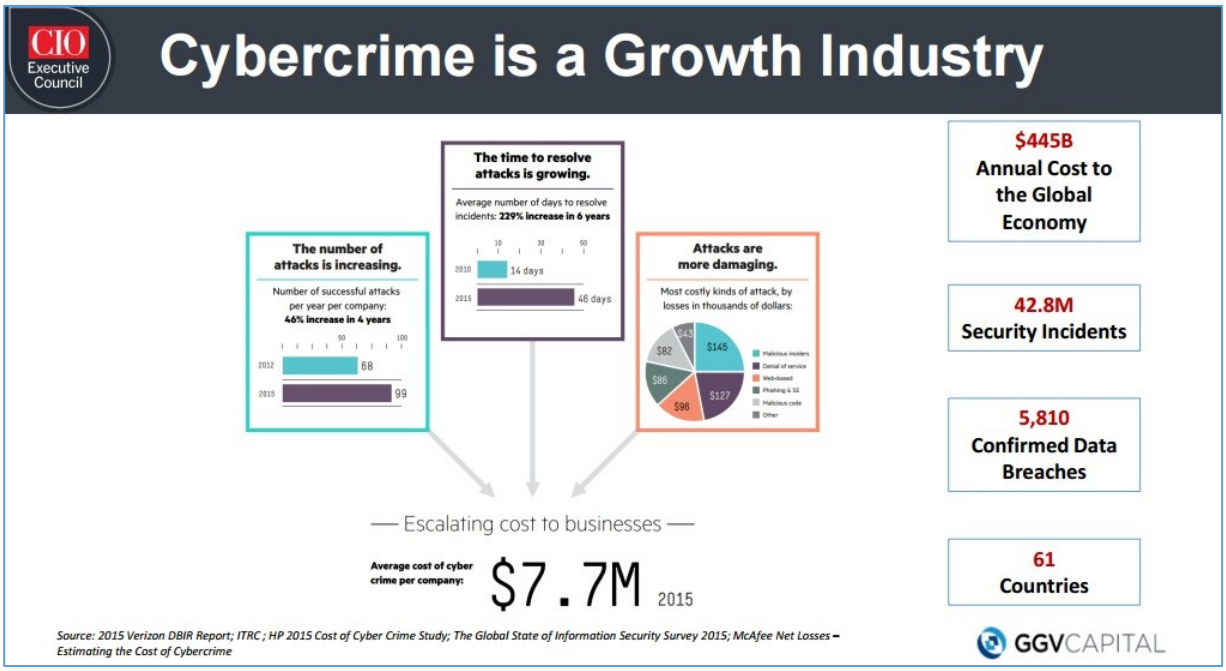
    1. **Strategic issues** also known as a risk profile: issues CIOs are going to have to address with the board or higher up;
    2. **Tactical issues**: address your organizations ability to meet the challenges of threats;
    3. **Operational aspect**: how is your current program effectively addressing your risk profile?

- Organizations should have a **Risk Appetite Statement**: this statement generally defines the temperature vs. how much resource capacity the organization is willing to invest in this problem. It is a building block that allows you to see what your next step will be.
- Overall, organizations need to have strong security, security policies, procedures and handling standards.



Types of Attackers:

- **Script Kitties**: Opportunist criminals, ones who target unpatched servers using generic exploits that circulate in Word and PDF files.
- **Focused Attacker**: Target certain type of information and look for whatever data they can get their hands on.
- **Highly Motivated Attacker**: These attackers are also known as APTs or Advanced Persistent Threats, people who have the main goal of targeting you and you alone.
- **Backdoor Attacker**: One who attacks from the inside, one who makes the organization question whether or not they have the protection or risk already inside.



What to Do In The Event Of a Breach:

Three steps in the Assessment process:

1. **Containment:** Understanding the degree of trouble is and be able to "stop the bleeding";
2. **Damage Assessment**: Ask yourself the questions of how bad is/was the problem? ;
3. **Post-Mortems**: Figure out how to prevent this from happening again in the same way.

Analytics and monitoring are good, but they are only a small piece of a large puzzle. Organizations need to understand their network understand what "normal" was before they implemented it.

- The most important thing that connects all these phases is **communication**: To whom am I communicating and when?
- **Transparency** is key: The sooner you are transparent outside of your organization the better off you're going to be regarding the external impact of protecting the branding.
- Don't be afraid to **include third parties**: Now is the time that speed is of the essence and organizations need additional perspectives that are not inside of their organization.

How to Balance the Benefit-Risk component:

- Organizations need to understand that no two organizations are alike; it all depends on what is the acceptable risk for your organization in having a complete network map of applications, platforms, and hardware that could help quickly analyze threats but is a risk in itself if it gets in the wrong hands.
- Organizations need to have information handy in a form that allows them to make decisions in a quick fashion.
- The key is to have a cyber-security program that can rapidly evolve at the speed of the business.

Final Thoughts:

***Mike Plantinga**, CIO, CIBC Mellon*

> "The maturity of the vendor governance and framework is going to be key to being successful in protecting data when it's no longer in the data center."

***Scott Angelo**, CIO, K&L Gates*

> "Don't be afraid to talk about flexibility. Security will change as often as the business requires us to change."

***Steve Ragan**, Senior Staff Writer, CSO Online*

"Learn from the past: take all the incident reports and look for patterns in the types of attacks you're seeing and threats you're facing. Use these as a stepping stone to go forward in your security program."

- Tim Scannell
CEC, Director of Strategic Content