www.pwc.nl

Information Security management in ICS / SG

For discussion purposes only

oktober 2012

pwc

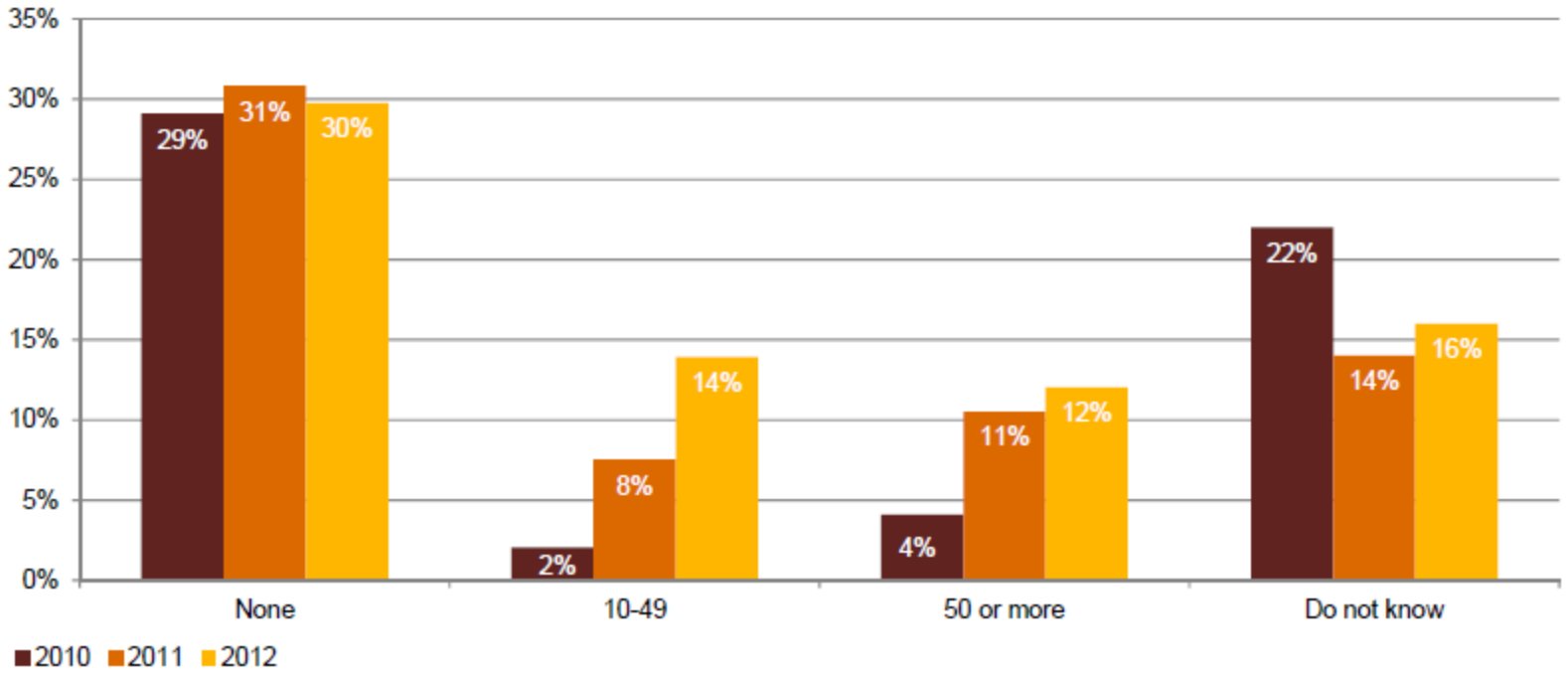
We live in a very safe world

Power and utilities companies that haven't detected *any* information security incidents during 2011.

Global State of Information Security Survey 2012, PwC

30%

Reported security incidents are on the rise though
Incident reporting in power & utilities



Question 17: "Number of security incidents in the past 12 months."

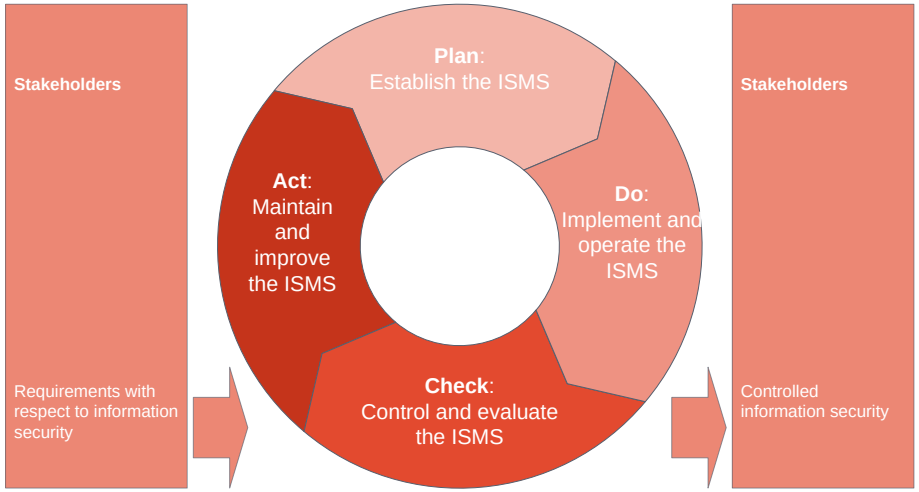
First of all: record and analyse your incidents

You should monitor your services and record incidents to be able to learn from them. Try to be innovative in monitoring and use all available information.

Information security management

Basically:

Making sure your controls match your business requirements.



Incident resolving at a financial institution
Real-life example (modified details)

A Denial of Service attack is taking place on on a large financial institution, targeting a vulnerability on an application server.

ISM is effective in many environments
Example: a centrally organised bank with standard infra

1. The Security Operations Center is notified that the internet channel is down. The incident is immediately confirmed and registered.
2. The Security Officer is informed and he assesses the situation together with the CIO, IT manager and specialists. It turns out that a vulnerability in a switch is exploited. Specialists advise to drop traffic from the originating IP. The Security Officer contacts the vendor of the app server software.
3. A new firmware version for the server software was already in the works in the standard cycle, testing is fast-tracked and the server is updated within 3 days. Extra monitoring takes place during these days.
4. As all information is recorded the incident can be analysed, threat profiles are updated and risk assessments are reviewed over the course of a month. The board agrees with all actions taken and provides extra funding for increasing infra redundancy.
5. Relevant (sanitised) details on the attack are shared with other banks in order to prevent future incidents.

Incident resolving in ICS / SG
Realistic scenario (modified)

A penetration test is performed on the production network of a utilities company, including the Programmable Logic Controllers.

An example based on real-life experience: PLC vulnerabilities

1. A vulnerability is discovered in a PLC type that drives pumping stations, where it fails when it is pinged. An incident is registered.

An example based on real-life experience: PLC vulnerabilities

1. A vulnerability is discovered in a PLC type that drives pumping stations, where it fails when it is pinged. An incident is registered.
2. The Security Officer is notified, and he talks to the IT manager. The IT manager does not acknowledge this is a problem as the production network is separated from the office automation network. No fix is provided.

An example based on real-life experience: PLC vulnerabilities

1. A vulnerability is discovered in a PLC type that drives pumping stations, where it fails when it is pinged. An incident is registered.
2. The Security Officer is notified, and he talks to the IT manager. The IT manager does not acknowledge this is a problem as the production network is separated from the office automation network. No fix is provided. The PLC vendor is contacted.

An example based on real-life experience: PLC vulnerabilities

1. A vulnerability is discovered in a PLC type that drives pumping stations, where it fails when it is pinged. An incident is registered.
2. The Security Officer is notified, and he talks to the IT manager. The IT manager does not acknowledge this is a problem as the production network is separated from the office automation network. No fix is provided. The PLC vendor is contacted.
3. The PLC vendor acknowledges the vulnerability. A patch will be included in the next release cycle.

An example based on real-life experience: PLC vulnerabilities

1. A vulnerability is discovered in a PLC type that drives pumping stations, where it fails when it is pinged. An incident is registered.
2. The Security Officer is notified, and he talks to the IT manager. The IT manager does not acknowledge this is a problem as the production network is separated from the office automation network. No fix is provided. The PLC vendor is contacted.
3. The PLC vendor acknowledges the vulnerability. A patch will be included in the next release cycle. Which is in 2013.

An example based on real-life experience: PLC vulnerabilities

1. A vulnerability is discovered in a PLC type that drives pumping stations, where it fails when it is pinged. An incident is registered.
2. The Security Officer is notified, and he talks to the IT manager. The IT manager does not acknowledge this is a problem as the production network is separated from the office automation network. No fix is provided. The PLC vendor is contacted.
3. The PLC vendor acknowledges the vulnerability. A patch will be included in the next release cycle. Which is in 2013.

Smart metering example: a patch may be available immediately, but updating all meters will take 6 months due to their volume.

An example based on real-life experience: PLC vulnerabilities

1. A vulnerability is discovered in a PLC type that drives pumping stations, where it fails when it is pinged. An incident is registered.
2. The Security Officer is notified, and he talks to the IT manager. The IT manager does not acknowledge this is a problem as the production network is separated from the office automation network. No fix is provided. The PLC vendor is contacted.
3. The PLC vendor acknowledges the vulnerability. A patch will be included in the next release cycle. Which is in 2013.
4. None of the information is recorded, the incident remains open until the fix is administered and is closed without additional details or analysis.

An example based on real-life experience: PLC vulnerabilities

1. A vulnerability is discovered in a PLC type that drives pumping stations, where it fails when it is pinged. An incident is registered.
2. The Security Officer is notified, and he talks to the IT manager. The IT manager does not acknowledge this is a problem as the production network is separated from the office automation network. No fix is provided. The PLC vendor is contacted.
3. The PLC vendor acknowledges the vulnerability. A patch will be included in the next release cycle. Which is in 2013.
4. None of the information is recorded, the incident remains open until the fix is administered and is closed without additional details or analysis.
5. None of the information is shared with other parties.

Lessons learned: a link to information security management

Organise information security.

Lessons learned: a link to information security management

Organise information security.

Focus on awareness.

Lessons learned: a link to information security management

Organise information security.

Focus on awareness.

Communicate with vendors.

Lessons learned: a link to information security management

Organise information security.

Focus on awareness.

Communicate with vendors.

Be aware of your infrastructural limitations.

Lessons learned: a link to information security management

Organise information security.

Focus on awareness.

Communicate with vendors.

Be aware of your infrastructural limitations.

Record, analyse and control.

Lessons learned: a link to information security management

Organise information security.

Focus on awareness.

Communicate with vendors.

Be aware of your infrastructural limitations.

Record, analyse and control.

Share and cooperate.

Lessons learned: a link to information security management

Organise information security.

Focus on awareness.

Communicate with vendors.

Be aware of your infrastructural limitations.

Record, analyse and control.

Share and cooperate.

Benchmark your organisation with the Global State of Information Security Survey

www.pwc.com

Information Security Management Systems
Standard ISO27001:2005 Deming cycle