CIO / CISO perspectives
Challenges and opportunities

Trond Ellefsen
Head of IT Statoil Development and Production North America
CISO keynote

1. Content and perspective
2. Common threats and the new Art of war
3. “Weapons of mass destruction”
4. Weapons of mass collaboration
5. The cloud, devices and OT
6. CISO role of 2013 and onwards
7. Q & A
2012 – a truly connected world with challenges

Almost everything and everyone is connected.

Devices are more prone to loss and theft containing potentially sensitive business data.

Enterprise applications & data must learn to coexist with personal apps & data.

The exposure is growing as a function of the speed of change and the "IT skills gap."

The Bottom Line from Sun Tzu: Victorious warriors win first then go to war, while defeated warriors go to war and then seek to win. Much Strategy prevails over little strategy!
Our planet is getting more Instrumented, Interconnected, and “Intelligent”

250 million
Almost 250 million smartphones were sold world-wide in 2010, surpassing laptop sales.

90%
Nearly 90% of innovation in automobiles is related to software and electronics systems.

10 billion
At the entrance to 2013, we expect there are 10 billion connected devices in the world, constituting an “internet of things.”

683 exabytes now,
Cloud traffic in 2016 will be 4,3 zeta bytes
Some spectacular cyber events

• 1982 – Stuxnets great grandfather – one of the alphabet agencies managed to blow up a Russian gas pipeline in Siberia by planting code that lead to systems overload and finally one of the largest non-nuclear detonations in the history.

• 1998 – Radar hack 1 – Allied forces hacked Serbian air defense systems blindfolding them so that air strikes against Kosovo became easier.

• 2001 Code Red – July 2001 computer worm infected more than 300,000 computers in the US

• 2003 Operation titan rain – Coordinated attack on public and private computer centers possibly with defense or industrial espionage background

• 2007 Radar-hack 2 – A targeted hacker attack towards Syrian air defense and radar system made it possible to bomb a military installation

• 2007 Web war 1 – A Russian and Estonian disagreement led to almost all net based systems in Estonia to stop

• 2008 Centcom A number of “unused” pin drives laying around led to a computer worm infected deep inside US military central command. The cleanup took 14 months

• 2009 GhostNet Spy software believed to be coordinated from the east systematically collected information from 103 countries IT systems.

• 2010 Stuxnet The manifestation of first real sophisticated cyber attack with addressing Siemens SCADA systems and producers of drivers.

• 2011 RSA secureID RSA secureID hacked to attack Lockheed Martin

• 2011 Shady RAT – Attack hit 72 organizations. Global cooperations, UN, IOC and weapons manufacturers.

• 2011 Duqu Stuxnets cousin, Mainly for information gathering.

• 2012 SaudiAramco and RasGas
Common threats

• 2010 Stuxnet - computer worm attacking Operational Technology (OT). Found on one computer in Statoil too.

• Night Dragon - a family of Trojan horses with origin the far east used to harvest information also from Statoil

• Increased tons of spoofed mail - mails with fake name of sender. Commonly used in spam and phishing e-mails, Facebook, IRS, eBay, FedEx.

• Social engineering - Identity theft - use other persons identity to commit fraud.

A Brief History Of Chinese Cyberspying

Chinese hackers steal critical oil player data

Hackers working in China broke into the computer systems of five multinational oil and gas companies to steal bidding plans and other critical proprietary information, the computer security company McAfee said in a report.

News wire - 10 February 2011 12:17 GMT

The report, which named the authors NightDragon, declared to identify the five known companies that had been hacked and published another news on a number of these breaches that could not be confirmed.
Critical national infrastructure is at risk when everything is becoming connected to everything else.
The new weapons of mass destruction

- History shows that when the human race make technological leaps, it first comes to use by the people in uniform. They no longer focuses all their energy on the “fire” element, but the 5th element, the internet is now becoming a true military warzone.
- Traditional civil approach to protect critical national infrastructure and operational technology (OT) might not scale to protect anymore.
- What we do not need are symbolic requirements that is outdated before they are on paper.
- What we need is collaboration across industry and government to ensure we understand the threat and can implement fit for purpose security. Compartmentalization when lightning strikes is on brick in the puzzle.
The new weapons of mass collaboration

• Our ability to connect to vast reservoirs of knowledge around the world will speed up the pace of technology change and increase our ability to solve some of the big challenges of our time.

• Our ability to balance security, risk and share information and will determine our ability to innovate and crack more of the remaining puzzles.

• To much security will hamper innovation and value creation facilitated by collaboration and social networks.

• To little security will destroy value creation.

• Balanced risk based security is the answer.
No time to talk we are moving our data to the cloud…
The cloud

• Admit it: The traditional security thinking of protecting is a difficult engineering task in this model. Determining if any particular cloud environment reliably provides stated levels of confidentiality, integrity and availability is even harder.

• Strategic recommendation 1: Determine Risk / Exposure tolerance for the data you want out there. Not everything belongs out there (yet)

• Strategic recommendation 2: Delay deployment of mission critical services until the required services, standards and controls are in place. However a lot can already be put out there.
Mobile devices

• Bring your own device (BYOD) is now a common phenomenon as the mobile device is increasingly a device that the user identifies themselves by. It is opening up the potential of productivity gains, serving as a stimulus for employee satisfaction and seeding innovation, while exposing the enterprise to data and device management risks.

• Strategic recommendation 1: Segmenting users into groups and apply access, awareness and support according to business risk profile.

• Strategic recommendation 2: Make it personal! Awareness building based upon peoples personal exposure gets their attention.
OT Operational Technology

• The worlds of IT and operational technology (OT) are converging, and IT leaders must manage their transition to converging, aligning and integrating IT and OT environments.

• Adopting pure IT technologies across operational technology (OT) introduces new IT security issues for OT organizations.

• With IT and OT converging, the scope of CIO/CISO authority may in need of planning and coordinating a new generation of operational technologies alongside existing information- and administration-focused IT systems.

• Strategic recommendation: CIO/CISO must assist OT organization in establishing the new common security perspective.
Operational Technology (OT)

- Strategic recommendation 1: Plan for that OT will predominantly be staffed by IT security people as pure IT takes over the proprietary “black box domain”

- Strategic recommendation 2: Aid in providing the oversight of IT+OT security requirements in a consistent, structured manner.

- Strategic recommendation 3: Understand the full architectural exposure. Mind the IT skills gap!
The new role of the CISO

• The CIO / CISO's role is becoming increasingly strategic as enterprise security matures and security functions become both more standardized and commoditized.

• The key skills required by a successful CISO are increasingly managerial, collaborative and communicative, rather than primarily technical. The ability to build consensus through translate it all into business risk and influence decisions is critical.

• Strategic recommendation 1: Translate IT and cyber risk from tribal IT language to business language risk and business impact.

• Strategic recommendation 2: As complexity grows architectural resources to support CISO and translate the full risk picture and exposure is essential.
Key takeaways

**Differentiation**
20/80 Focus on your crown jewels. Protect what is most important

**Architecture**
Holistic understanding is required for understanding the full technological risk exposure. This requires architecture skillset

**Awareness**
Make it personal

**Balance**
Balance security and rules and don’t let our fear come in the way of letting us utilizing the reservoir of knowledge

**The “vault”**
20% of the data should maybe not be in the cloud for now

**BUSINESS VALUE**
Q&A

Trond Ellefsen
BA CIO
Development & Production
Statoil North America
trell@statoil.com
Tel: +1 713 966 9240
www.statoil.com
There’s never been a better time for good ideas