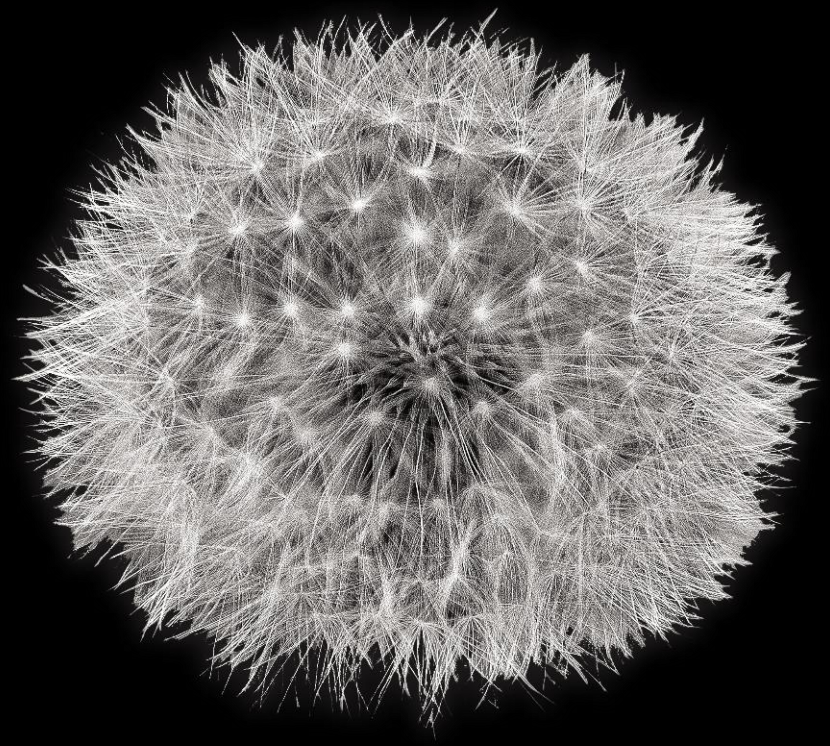
Deloitte.



Fondsmæglerforeningen

Ole H. Madsen, Juni 2019

”Den finansielle service Industry er en af de sektorer, der oftest udsættes for Cyber angreb. Hovedparten af truslerne stammer fra kriminelle og nationalstater, der ønsker at udnytte eller tjene på data, der anvendes af den finansielle organisation.

I indlægget vil vi beskrive udfordringerne for Cyber sikkerheden i Danmark, vi vil tale om motiver, taktikker og teknikker for angreb indenfor den finansielle sektor, samt diskutere praktiske tiltag for hvordan vi kommer i gang med at beskytte os som organisation.”

Presentation
Ole Haugaard Madsen

- Headed compliance, security and quality organisations with teams in Europe, China, South Africa and the Philippines
- CSO (Chief Security Officer), CISO (Chief Information Security Officer) and Quality/Process in service organisations
- Clients in Europe, China and the US
- Certified, audited and conducted due diligence of organisations within many different industry standards and best practices
- Owned ISO27001, ISO9001 and ISO20000 certificates
- Designing processes and delivery models for large governance risk and compliance business units

Hvor mange ansatte er I i Jeres organisationer?

Hvor mange af Jer har været ramt af et Cyber incident?

Hvad er det for type Cyber risks I er eksponeret for?

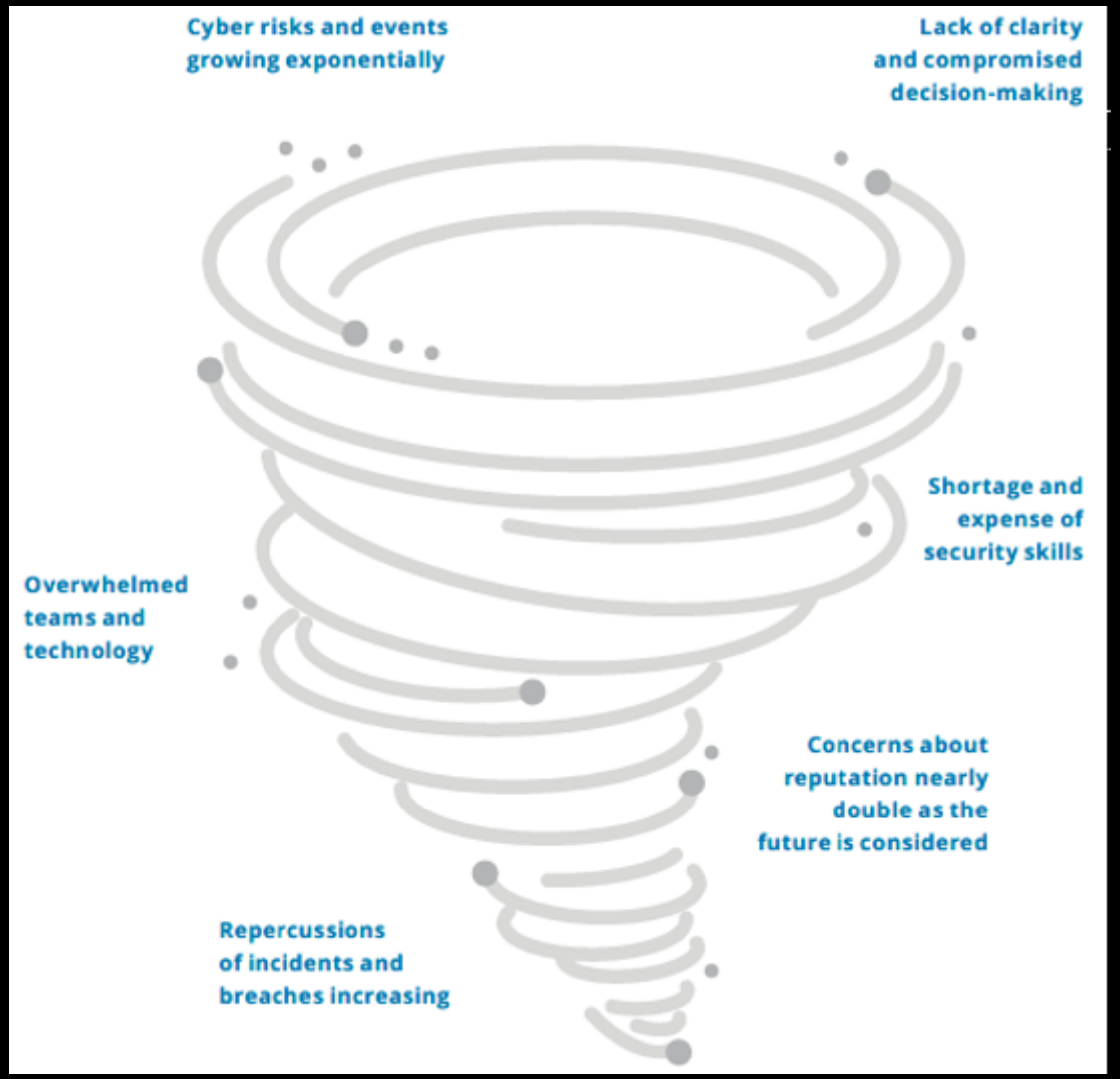
Agenda

1. Den ”perfekte storm”… – vi er påvirket af mega-trends

2. Motiver, taktikker og teknikker for angreb indenfor den finansielle sektor

3. Praktiske tiltag for hvordan vi kommer i gang med at beskytte os som organisation

Den ”perfekte storm”… (1/2)



Den ”perfekte storm”… (2/2)

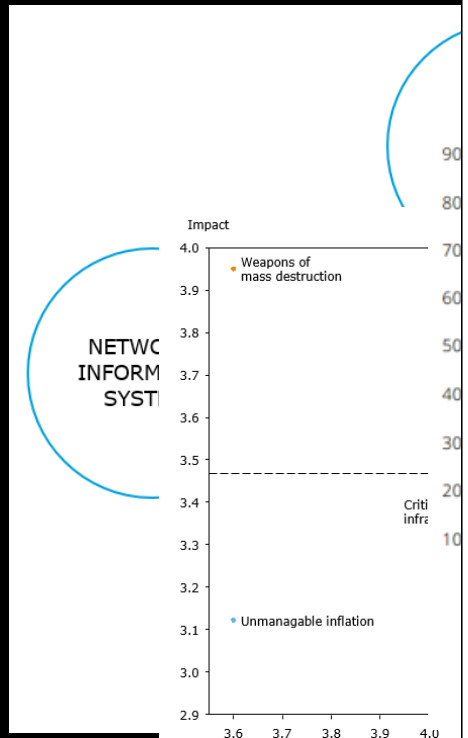
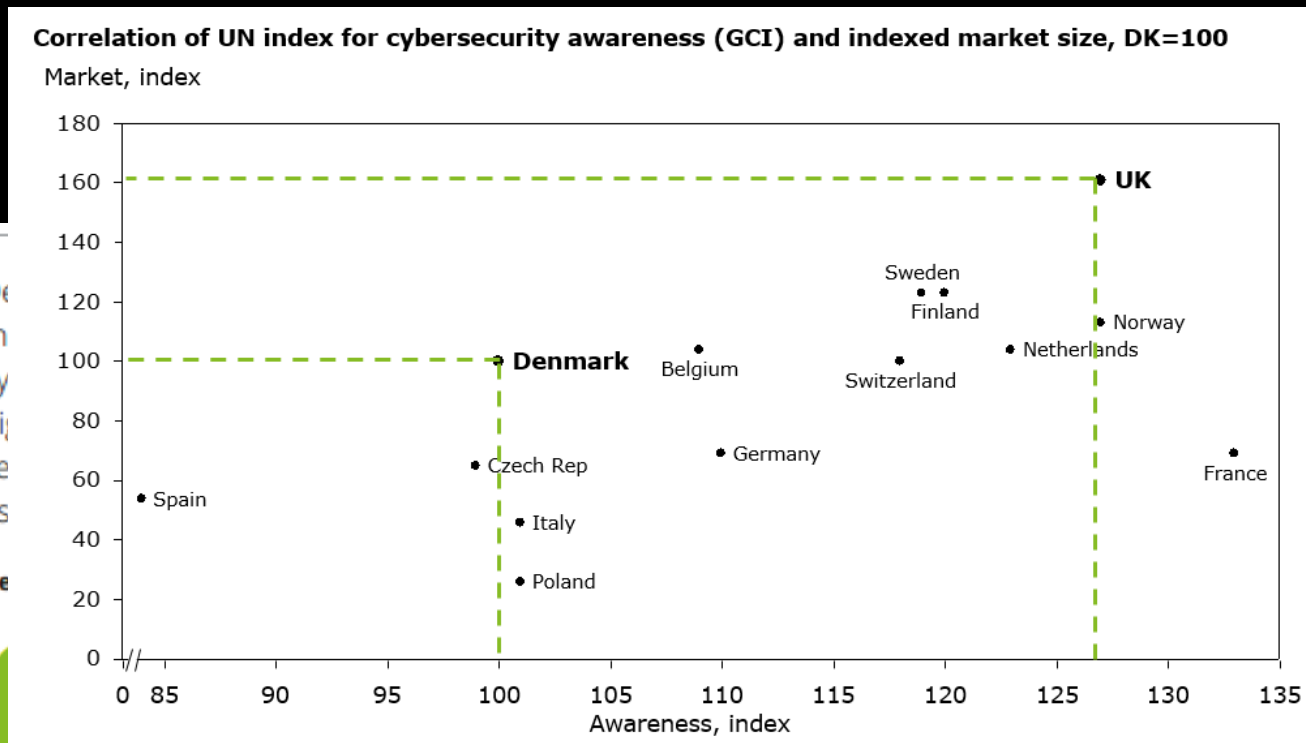


Table 1. Number of devices per household

2012	2017	2022
8 devices	23 devices	50 devices
• 2 smartphones	• 4 smartphones	• 4 smartphones
• 2 laptops/ computers	• 2 laptops	• 2 laptops
• 1 tablet	• 2 tablets	• 2 tablets
• 1 DSL/cable/fibre/ Wi-Fi modem	• 1 connected television	• 3 connected televisic
• 1 printer/scanner	• 2 connected set-top boxes	• 3 connected set-top boxes
• 1 game console	• 1 network-anchored storage	• 2 e-Readers
	• 2 e-Readers	• 1 printer/scanner
	• 1 printer/scanner	• 1 game console
	• 1 game console	• 1 smart meter
	• 1 smart meter	• 3 connected stereo systems
	• 2 connected stereo systems	• 1 energy consumptic display
	• 1 energy consumption display	• 2 connected cars
	• 1 internet-connected car	• 7 smart light bulbs
	• 1 pair of connected sport shoes	• 3 connected sport devices
	• 1 pay-as-you-drive device	• 5 internet-connectec power sockets
		• 1 connected weight
		• 1 eHealth device
		• 2 pay-as-you-drive d
		• 1 intelligent thermostat
		• 1 network-attached storage
		• 4 home automation sensors

Source: OECD "Digital Economy Outlook 2015".



Motiver, taktikker og teknikker for angreb indenfor den finansielle sektor

Executive summary

Nuance Power
PDF Document

The Financial Services Industry (FSI) is likely one of the most targeted sectors due to its immediate and direct relevance for financially motivated threat actors. The majority of threats stem from criminals of varying sophistication and nation-states as they seek to exploit or monetize data held by FSI organizations

Threat actors	Motives	Core threats
Criminal syndicates	**Financial gain**: Cyber criminals with varying degrees of sophistication target FSI to monetize data by the sector	Targeting of Bank Networks
Advanced Persistent Threats (APT)	**Fraud:** A core threat to the FSI industry is driven fraud-enabling malware and tools. Banking trojans, info-stealers and account checkers constitute core components of these threats.	Targeting of Insurance & Real Estate Companies
Carders and "Script Kiddies" (Skidz)	**Cyber espionage:** State-sponsored adversaries typically target data such as business strategic plans goals, finance documents or product description from FSI organizations, as well as customer specific information.	Espionage Threats
		Fraud-driven Threats
		Ransomware and other Cross-industry Threats

Observation 1 | Targeting of Bank Networks

Deloitte CTI continues to observe significant targeting of bank networks from criminals and state-affiliated groups.

Threat actors

APT groups and criminal syndicates: Multiple adversaries have the sophistication to successfully target bank networks. During 2019, prominent campaigns impacting banks were affiliated with EmpireMonkey and TA505.

Threat motivator

Financial Gain: Criminals seek to compromise banking networks and leverage their access to conduct large-scale fraudulent transactions.

Tactics, techniques, and procedures

Threat actors leverage various means to compromise banks. **Spear-phishing emails with malicious attachments**, such as Microsoft office documents with macros, are extremely common. These typically deliver **Remote Access Trojans (RATs)** that allow adversaries to exfiltrate information. Many adversaries also use living off the land techniques, exploiting native Windows tools to achieve their objectives.

Observation 2 | Targeting of Insurance & Real Estate companies

Transactional information and Personal Identifiable Information (PII) held by insurance and real estate companies is of interest to criminals.

Threat actors

Cyber criminals and syndicates: Sophisticated criminal groups such as Cobalt Gang target insurance companies consistently. Threat actors are also actively obtaining access to real estate companies in multiple regions.

Threat motivator

Financial Gain & Fraud: Insurance and real estate companies hold transactional information that can be monetized by threat actors that are motivated by financial gain. Similarly, they hold vast amounts of Personal Identifiable Information (PII), which can facilitate identity theft.

Tactics, techniques, and procedures

Adversary leverage **Remote Access Trojans (RATs)** and **info-stealers** typically delivered via emails against insurance and real estate companies. Credential Stuffing attacks that exploit factory default credentials have also been observed.

Observation 3 | Espionage threats

The FSI industry holds data that is of demonstrable interest to numerous nation states which constantly target the industry to conduct cyber espionage.

Threat actor

APT groups: Nation-state groups have the resources and incentives to persistently target FSI organizations with advanced, customized malware.

Threat motivator

Espionage: State-sponsored adversaries typically target data such as business strategic plans & goals, finance documents from FSI organizations, as well as customer specific information related to high-priority intelligence targets. As an example, Chinese APT groups have targeted FSI organizations during Merger & Acquisition negotiations with State-owner Chinese enterprises.

Tactics, techniques, and procedures

APTs typically pursue their objectives over an extended period of time ranging from months to years. APTs leverage **sophisticated, customized malware** to achieve their objectives, and they adapt to their operating environment, including changes in their target's defense posture. In addition, they will **persistently target the same victim** until their objectives are accomplished. By remaining hidden in a compromised environment for extended periods, APTs also pose a significant threat to an organization's intellectual property and proprietary technologies, due to their advanced data exfiltration capabilities.[12]

Observation 4 | Fraud-driven threats

Given its clear and direct relevance to financially motivated adversaries, fraud-driven threat actors have targeted the FSI since its inception.

Threat actors

Cyber criminals: The cybercrime ecosystem enables threat actors of lower sophistication to overcome the barriers of entry by supplying them with malware capabilities from developers with advanced skills.

Threat motivator

Financial gain: Fraud enablement by collecting the credentials of online banking customers, credit card numbers and other data such as PII that can be used to conduct fraud.

Tactics, techniques, and procedures

The **malware threats** that facilitate this broadly fall into the categories of **banking trojans**, **malware focused** on the collection of payment card information, info-stealers and account checkers. Across these threats, certain malware implants are adept at bypassing common enterprise defenses. Coupled with advanced social engineering, these threats pose the greatest risk to the FSI sector.

Observation 5 | Cross-industry threats

Ransomware, RATs and supply chain threats constitute the major cross-industry threats facing FSI.

Threat actors

Cyber criminals: Adversaries of both low and high sophistication leverage ransomware and RATs. Supply chain threats generally stems from threat actors with advanced capabilities such as state-sponsored APT groups, or organized criminal groups.

Threat motivator

Financial Gain: Profit is the primary motivator from ransomware and RAT threats. Supply chain compromises may be leveraged by more sophisticated adversaries aiming to deliver ransomware or RAT geared toward espionage operations.

Tactics, techniques, and procedures

Phishing emails, of varying quality, are often used to compromise specific targets with RATs and ransomware. Scripting is often leveraged to compromise victims, e.g. **Office documents with Macros**. PowerShell is consistently used by a multitude of threat actor to deliver, execute and achieve persistence for their RAT payloads. Supply chain compromise involves the manipulation of products or product delivery mechanisms to introduce malware threats via a third party.

Praktiske tiltag for hvordan vi kommer i gang med at beskytte os som organisation

Hvilke 10 fejl ser vi virksomheder burde have forberedt NÅR de har været angrebet

Error #1
Rushing

- Restoring infected system without securing evidence
- Unsecure Logon to infected systems
- Shut down of critical systems

What you think you do:

What you actually do:

Error #2
Vague or missing Roles

- Lack of a clear “Chain of Command”
- Lack of (Major) Incident Manager
- Appointing the Operation Lead as Incident Manager.
- Forgetting a “Practical-coordinator” role – e.g. food, coffee, sleep, extra monitors, whiteboards
- Top executives getting briefings straight from the Handler on the floor

Error #3
The Lone Ranger…

- Quote: ”I thought I could do it – I had read about it in the news”
- Lack of training and experience – but high on confidence
- Afraid of telling ”the grown ups” (CFO/CEO/DPO)

Error #4
Forgetting compliance

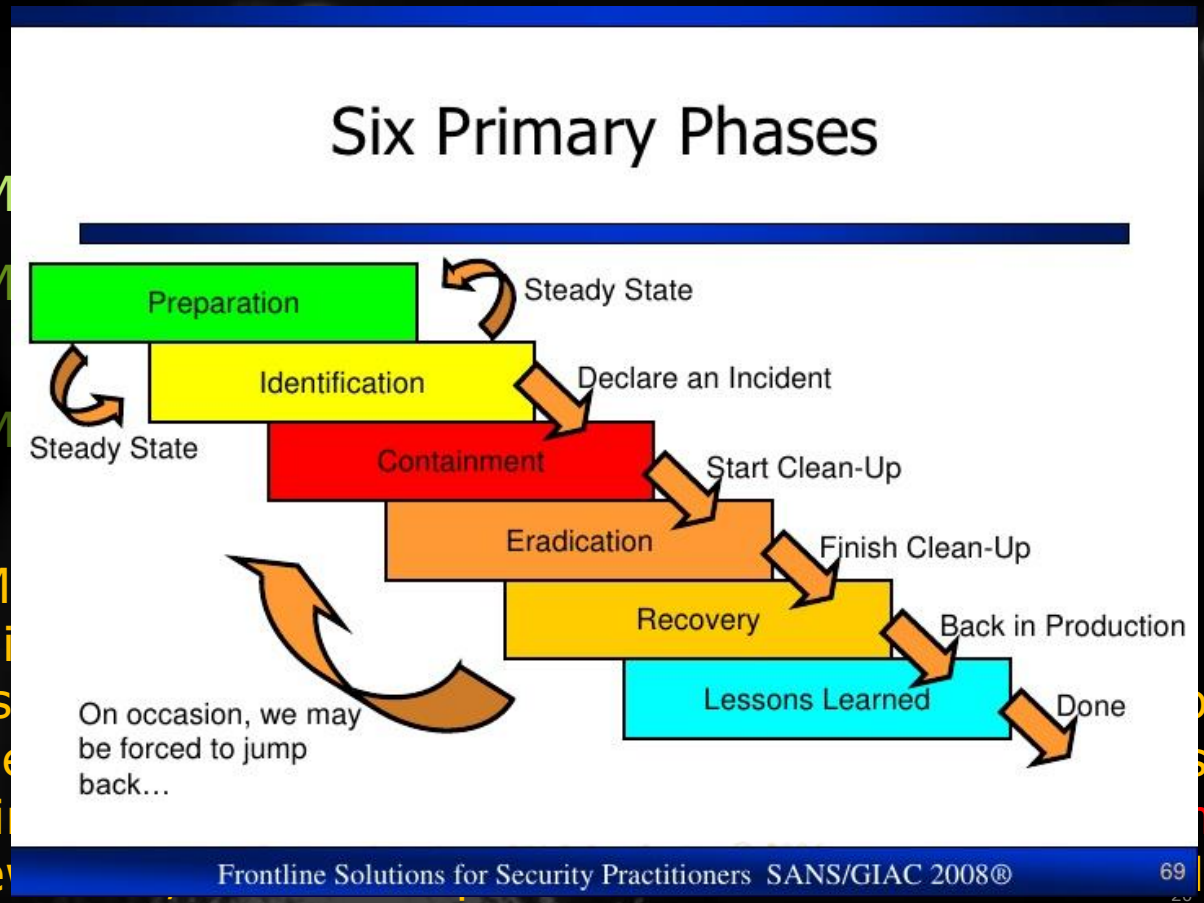
- First responders don’t often think of Compliance - GDPR and other regulations
- IT personnel are not trained in compliance
- Identification of lost data is often forgot
- Customer contracts and SLA’s

Error #5
Premature shift from Identification to Eradication

- Often responders think the first possible treatment is the right one.

Simple question: What was the machine hit by?

- Ransomware…
- Ransomware of type X
- Ransomware of type X, lateral moved from M
- Ransomware of type X, lateral moved from M Z.
- Ransomware of type X, lateral moved from M Z. Machine Y is still infecting new machines.
- Ransomware of type X, lateral moved from M (DA-Z). Machine Y is still infecting new machi ago via a open RDP service. DA-Z have acces engineering department over a period of 3 we data have been exfiltrated. DA-Z have been i systems, pulled a golden ticket, created 1 ne



Error #6
Unclear/Incorrect/Nonexciting Communication

- Quote: ”We think we know what hit us, and got it almost under control”, executive briefing 45 minutes before they had to shut down production and rebuild from backup (#5)

  - a now former CIO

- Briefings of Top Management or shareholders before a containment-plan is ready
- Briefing of clients/customers without a strategy and real preparations
- Silence

Error #7
Top Micro-Management

- Over-involvement of top Management in crises
- Lack of trust to the Crisis team makes the top leaders take charge
- Top leaders making operational decisions in haste (#1)

Error #8
Forgetting the ‘Lessons Learned’

- Focusing on the culprit rather than the real cause
- “Now we know. Lets do it better next time”-culture
- Top Management expect technical solutions to fix it all
- Fixing only the symptoms

Error #9
Redesigning IT-architecture during the fire

- Making major changes when under pressure is often not ideal. Segregating WLANS (for the first time), moving production to Cloud, changing firewall-vendor or deploying new hardened server images often something which need some through planning
- Upgrading to the newest OS often come with more trouble than predicted

Error #10
Not Sleeping enough

- Anything you do after 18 hours of work is often a bigger risk than the initiating incident
- Most ideas you get after 24 hours of work are just waiting for the Darwin award
- Compensating lack of sleep with Energy drinks/coffee

Top 10 mistakes often committed by companies under attack

1. Rushing
2. Vague or missing Roles
3. The Lone Ranger
4. Forgetting compliance
5. Premature shift from Identification to Eradication
6. Unclear/Incorrect/Nonexciting Communication
7. Top Micro-Management
8. Forgetting the ‘Lessons Learned’
9. Redesigning IT-architecture during the fire
10. Not Sleeping enough

Deloitte.