2021-11-03

Digitalisering av kraftbransjen – Cybersikkerhet rundt stordatahåndtering

cybersikkerhet i kraftsektoren Nov 2021

Mohammad M R Chowdhury, PhD, Principal Designer, Network Cyber Security & IT, ABB PA Energy Industries

Associate Professor University of Oslo

Digitalisation in the energy sector

Digital components

Different sensors in wind turbines give away information about the condition of various components Detect, monitor, communicate…

Rich cloud platform

Centralized control

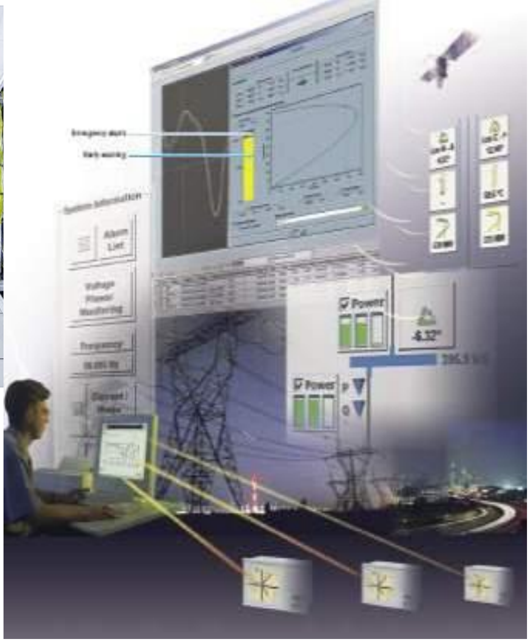
Remote monitoring

Advanced services

“Digital” Power lines

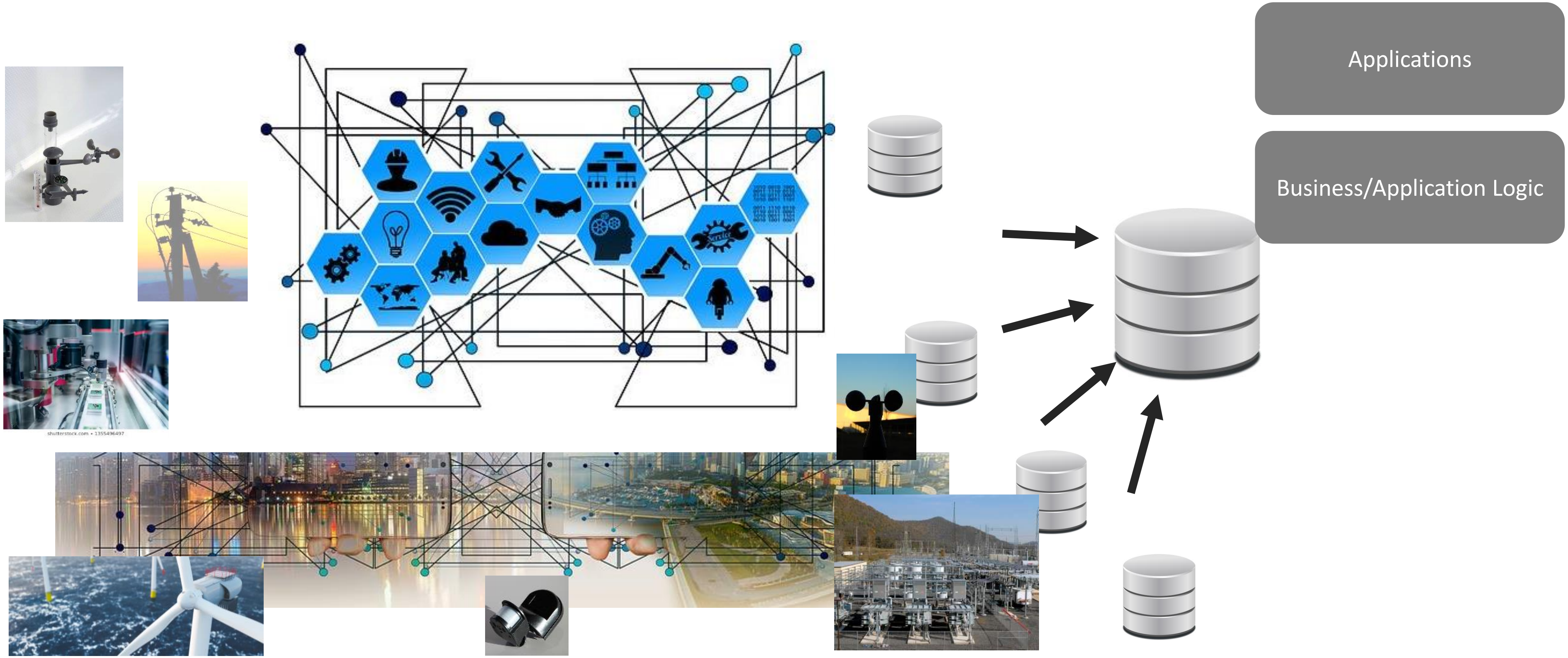
Sensors along the power lines measure temperature, vibration, icing, the angle of inclination of the lines.

Real-time ‘Digital’ SCADA



Sensors in all stages of the value chain – for optimization of energy systems

Digitization to Big data

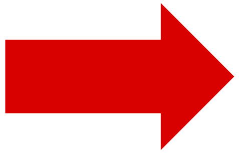


Applications

Business/Application Logic

Renewable - distributed data source

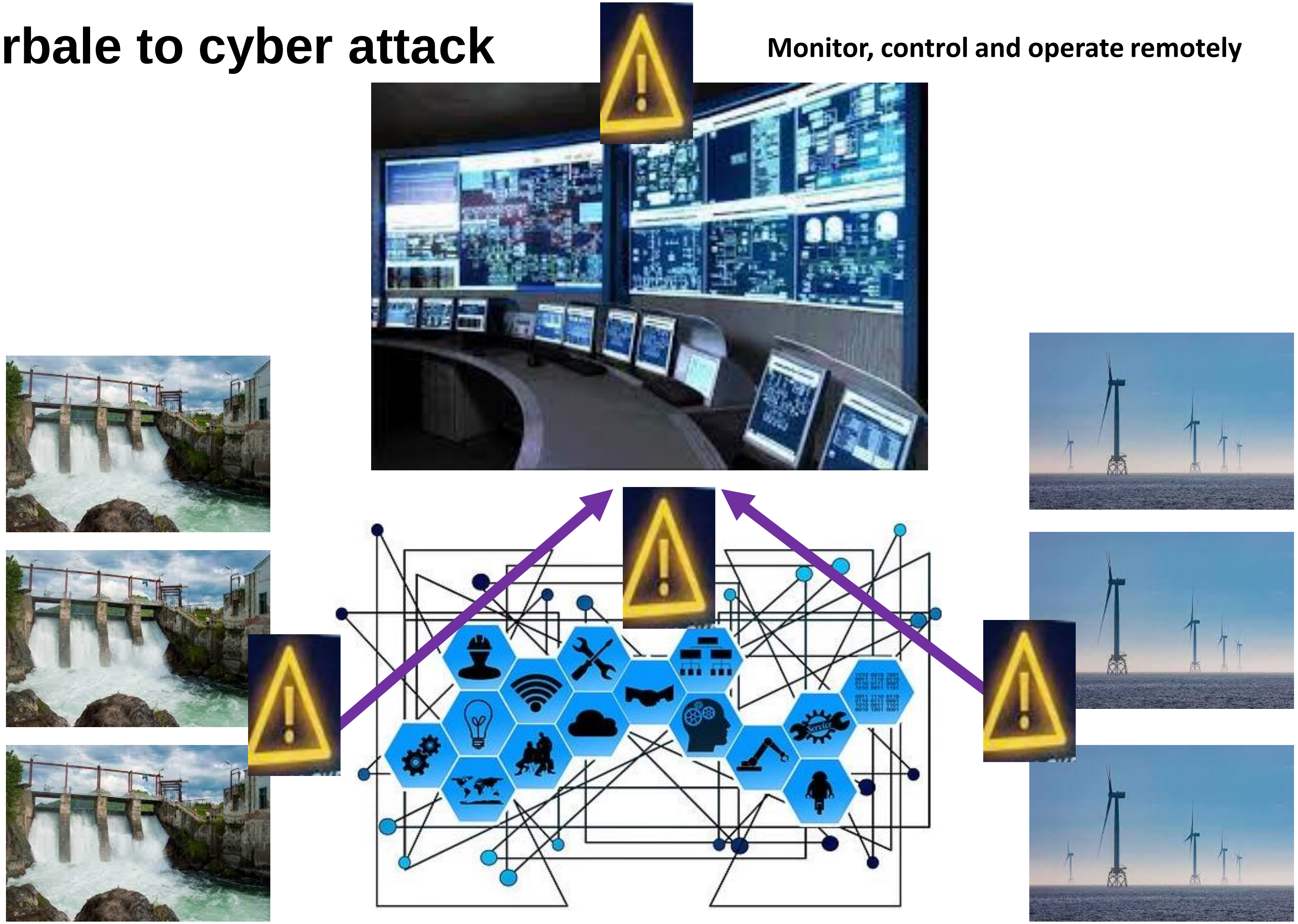
Fossil fuel
Localized



Renewable
More distributed

- Increase use of ICT
- Unmanned
- Increase of monitoring
- Centralized control
- Predictive maintenance

More vulnerbale to cyber attack



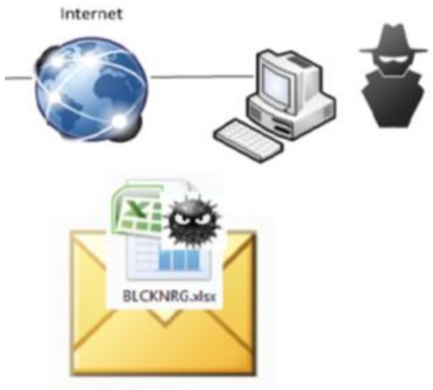
Monitor, control and operate remotely

Unmanned
Distributed remotely

Increase use of ICT

Risk

RISIKO:
Threat actors gain access to data, they establish an image of the power system and understand how to carry out a targeted attack. The threat actors always find the weakest link.

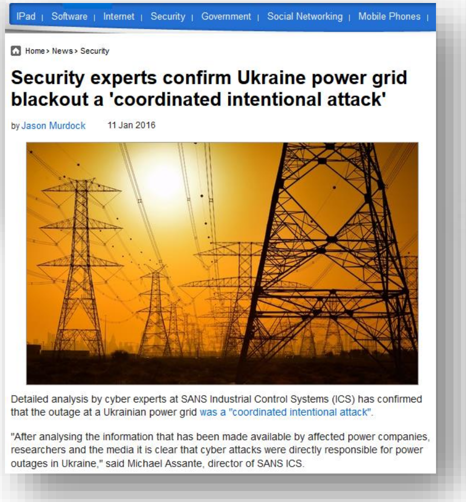


```
nForest.sweep(verbose);
(int i = 0; i < mainAgents.length; i++) {
mainAgents[i].sweep(verbose);

>= maxT) {
System.out.println("Password");
break terminated;

rest.shouldTerminate()) {
out.println("F = empty");
```

Cyber Attack!

Destroy
industrial
process

Cause power outage



IPad | Software | Internet | Security | Government | Social Networking | Mobile Phones |

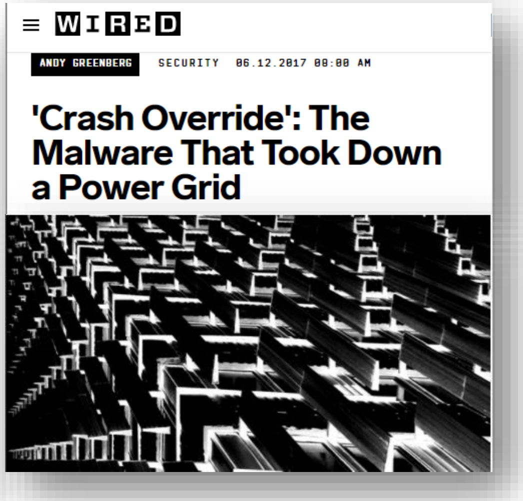
Home > News > Security

Security experts confirm Ukraine power grid blackout a 'coordinated intentional attack'

by Jason Murdock 11 Jan 2016

Detailed analysis by cyber experts at SANS Industrial Control Systems (ICS) has confirmed that the outage at a Ukrainian power grid was a "coordinated intentional attack".

"After analysing the information that has been made available by affected power companies, researchers and the media it is clear that cyber attacks were directly responsible for power outages in Ukraine," said Michael Assante, director of SANS ICS.

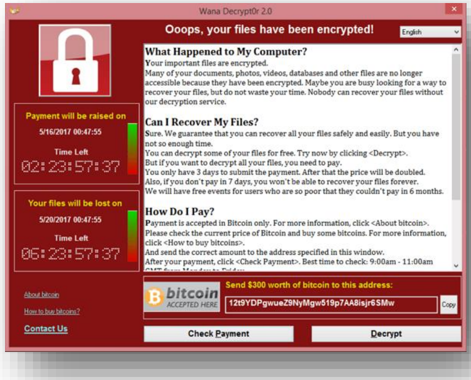


WIRED

ANDY GREENBERG SECURITY 06.12.2017 08:00 AM

'Crash Override': The Malware That Took Down a Power Grid

Ransomware



Ooops, your files have been encrypted!

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

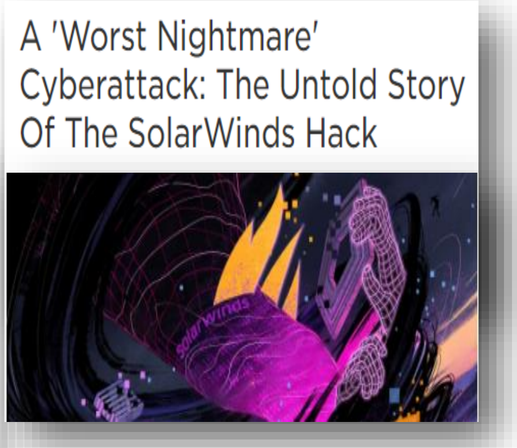
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Supply chain
attacks



A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack

"This release includes bug fixes, increased stability and performance improvements."

Sources:
https://www.wired.com/story/crash-override-malware/, https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack

The Energy Industry - The Threat and Events

2006 – Black Energy 1 - DDoS tools

2010 – Black Energy 2 – Vider developed to include spying tools and spam tools

2011 – Night Dragon – Sickened cyberattacks targeting sensitive information in the energy industry

2013 – Havex malware – Cyber espionage aimed at the bla energy industry

2014 – Black Energy 3 – Further developed with the ability to access SCADA networks

2015 – Cyberattack: Malware infects 3 regional energy companies and is used in a coordinated attack

225,000 customers without power for up to 6 hours

2016 – Industroyer/CrashOverride malware designed to attack the electrical grid

2016 – Cyber attack: automated attack (Industroyer) causes power bride in a big city

760,000 customers without power for 1.5 hrs

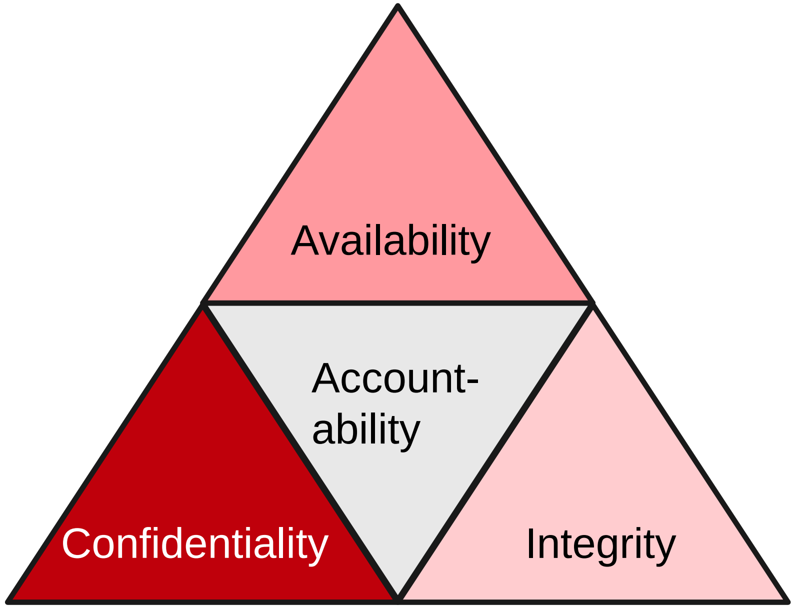
2016 – Now – Ongoing intrusions in the energy sector

2020 – Cyber attack: - Solar Winds – supply chain attack

2021 – Cyber Attack: - Volue RYUK Ransomware Attack

Cybersikkerhet – hva er det?

Cybersecurity – securing physical infrastructure and physical things that are vulnerable via ICT



"CIA triad" + Accountability:

Confidentiality – preventing access for unauthorized persons

Integrity - Prevent alteration/deletion by unauthorized persons

Availability – ensuring availability at all times for the authorized users

Traceability – to be able to document the course of the event retrospectively with temporable responsibility

Cybersecurity in practice

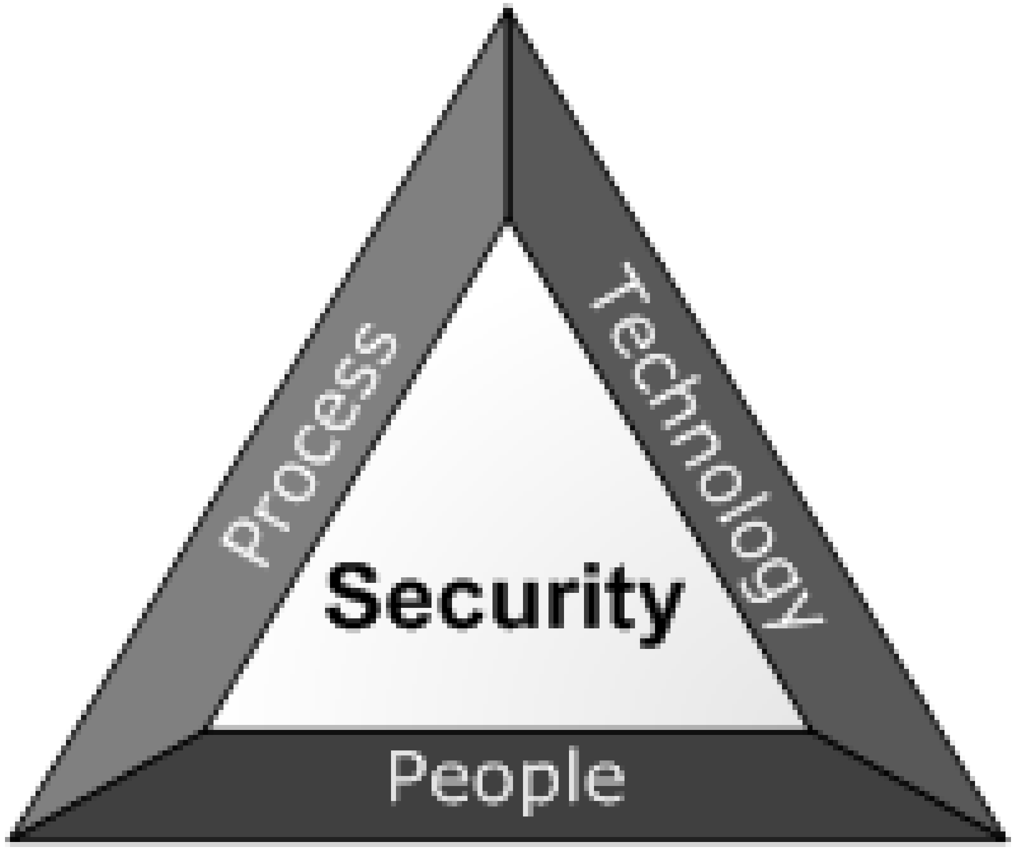
Identify

Protect

Detect

Responders

Restore



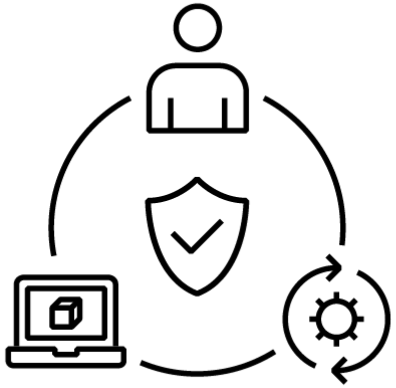
- Risk assessment
- Asset Inventory
- Perimeter Defense
- Network Segmentation
- Access Control
- Secure Remote Access
- System Integrity and Availability
- Software Management
- Hardening
- Security Awareness & Training
- Event & Incident Management

Cyber security – a life cycle management

It is important to engage and educate people, develop and implement processes, and design and deliver protected technology

3 Components:

- Humans, Processes, and Technology: Each of these must be activated to protect digital systems



Human

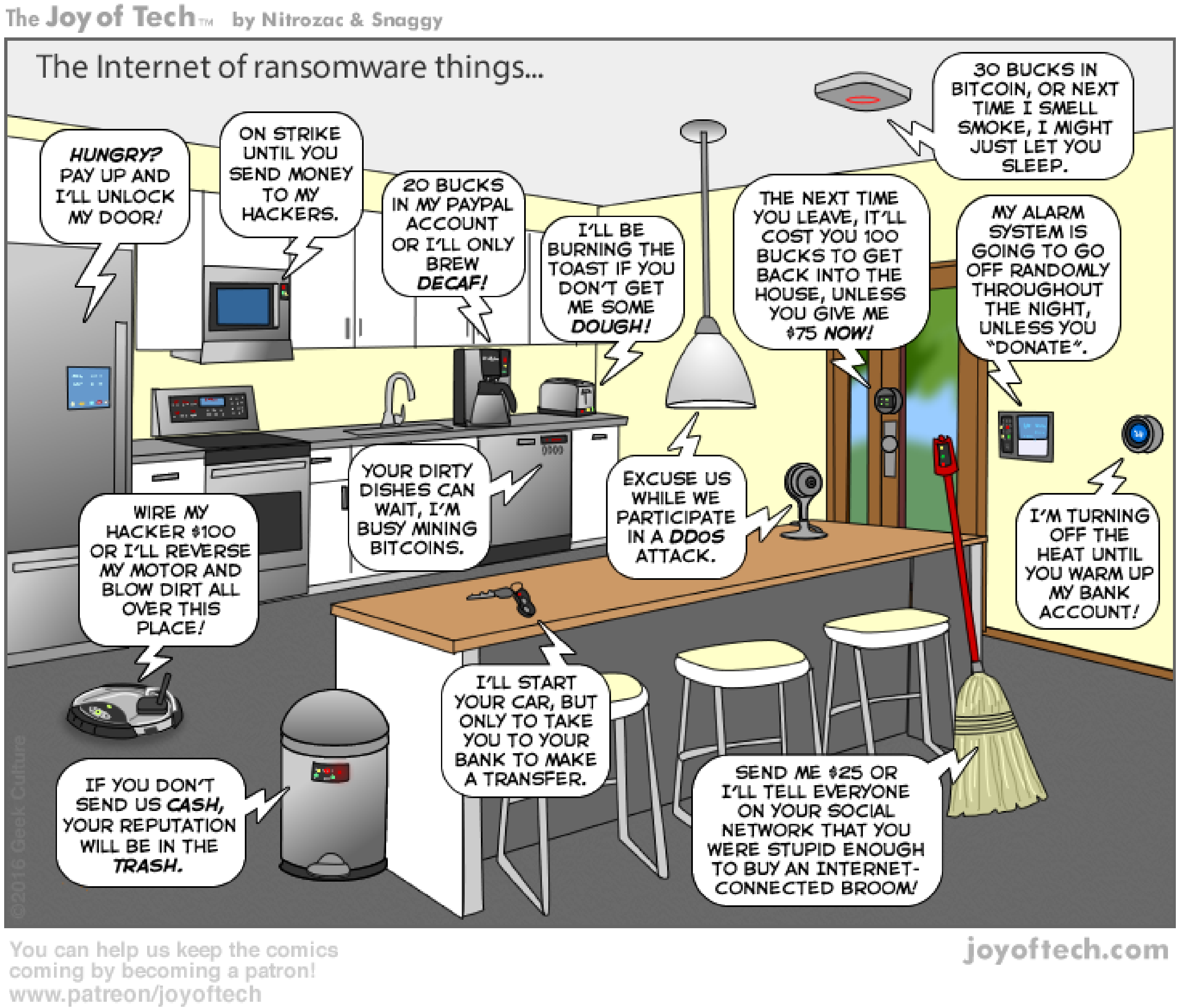
- Humans are critical to being able to prevent and safeguard against cyber threats.
- Organizations need competent people to implement and take care of cyber security measures (technology and process).

Processes

- Policies and Procedures are a necessity for the organization's effective security strategy.
- These must be able to change in line with changes in the threat picture.

Teknology

- Technology is important for preventing and mitigating cyber risk.
- Technology depends on people, processors and procedures to mitigate risk.


The Joy of Tech™ by Nitrozac & Snaggy
The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
EXCUSE US WHILE WE PARTICIPATE IN A DDOS ATTACK.
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
©2016 Geek Culture
You can help us keep the comics coming by becoming a patron! www.patreon/joyoftech
joyoftech.com

ABB