Incident response in the energy sector

Margrete Raaum,
Statnett SF and
FIRST, Forum of Incident Response and Security Teams

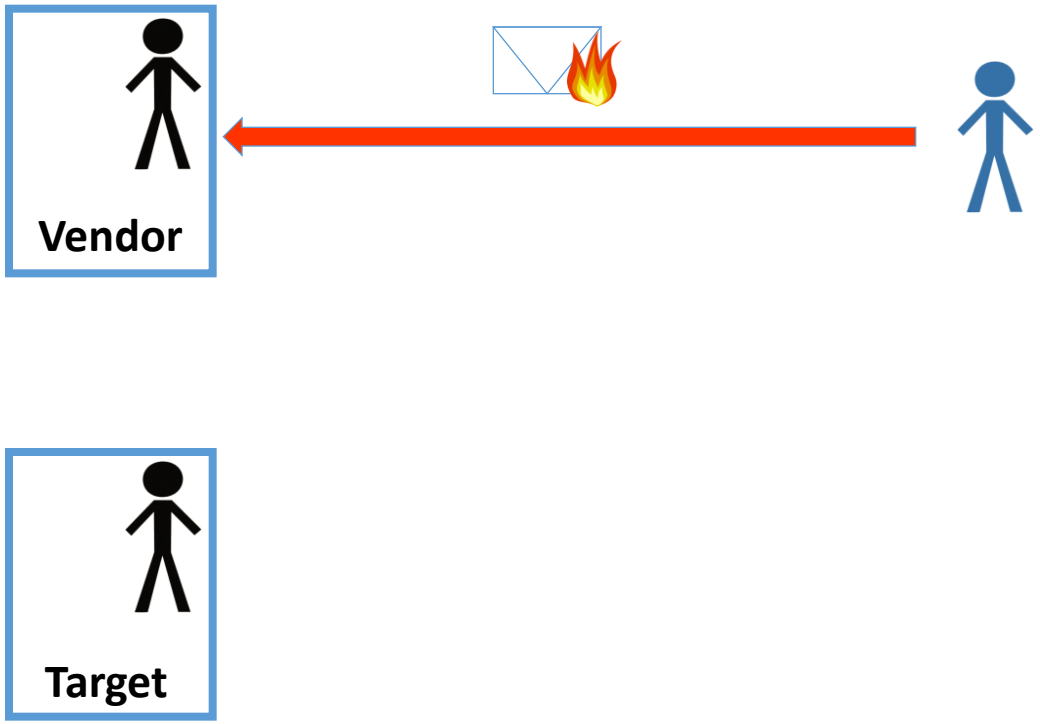
4SICS, October 23. 2014

Statnett

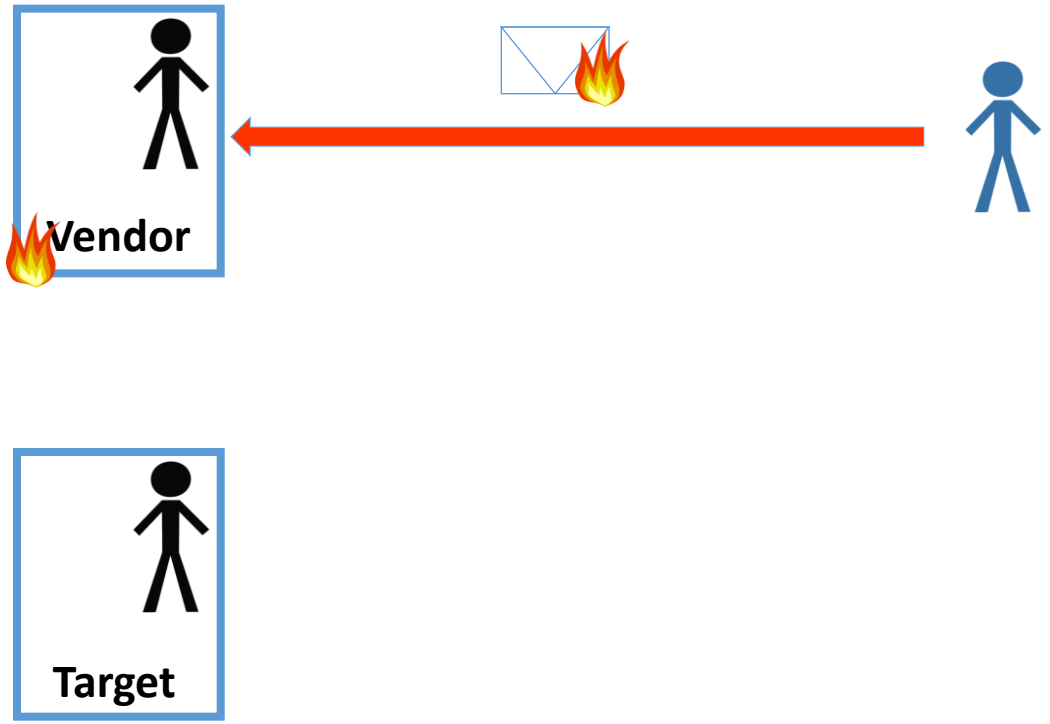
Incident response

- IR is more than just a characterization of an incident, it includes analysis
- Many companies are reluctant to share incident data because of reputation or fear of repercussions from the regulatory authority
- Unfortunately this is a policy that hinders good incident response

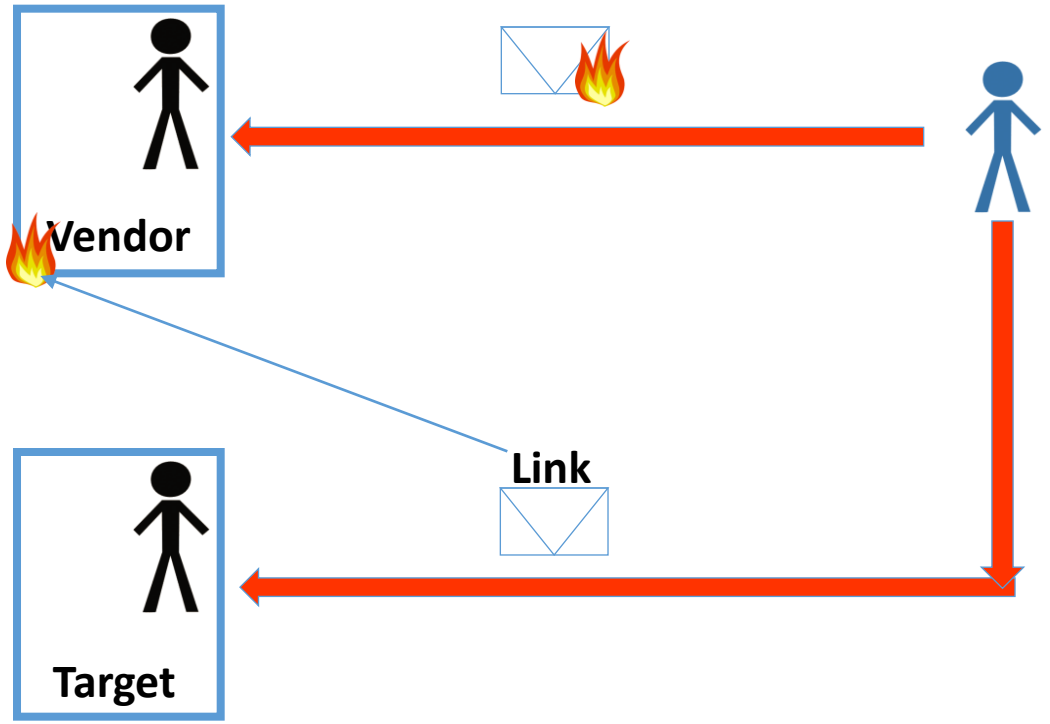
Combination attacks



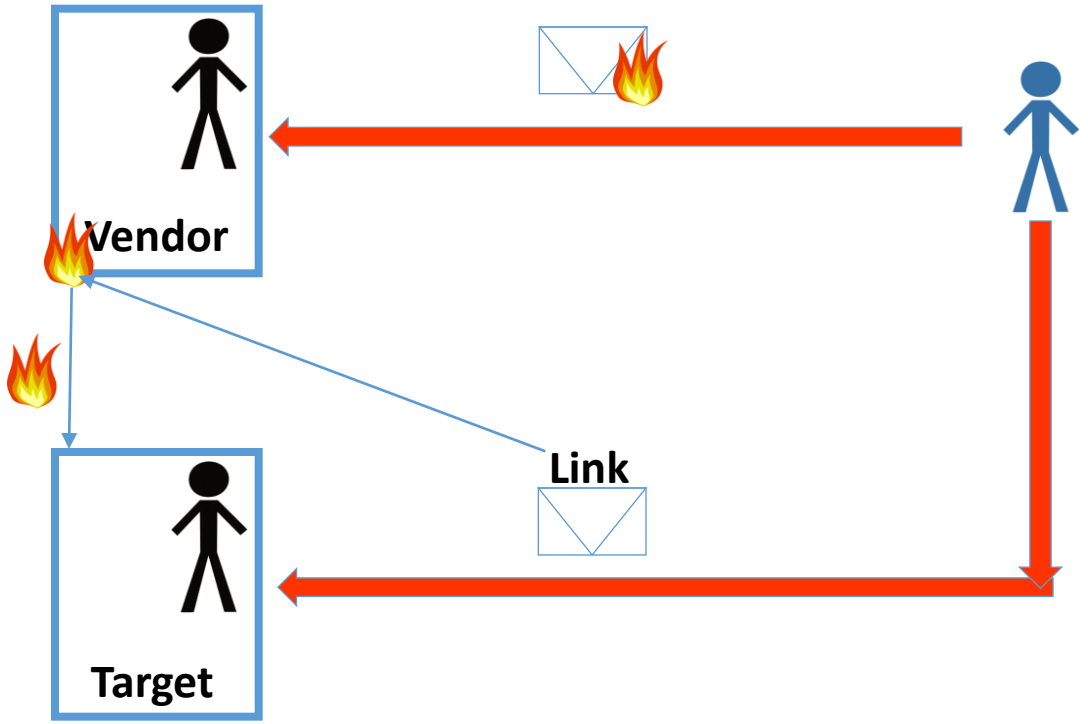
Combination attacks



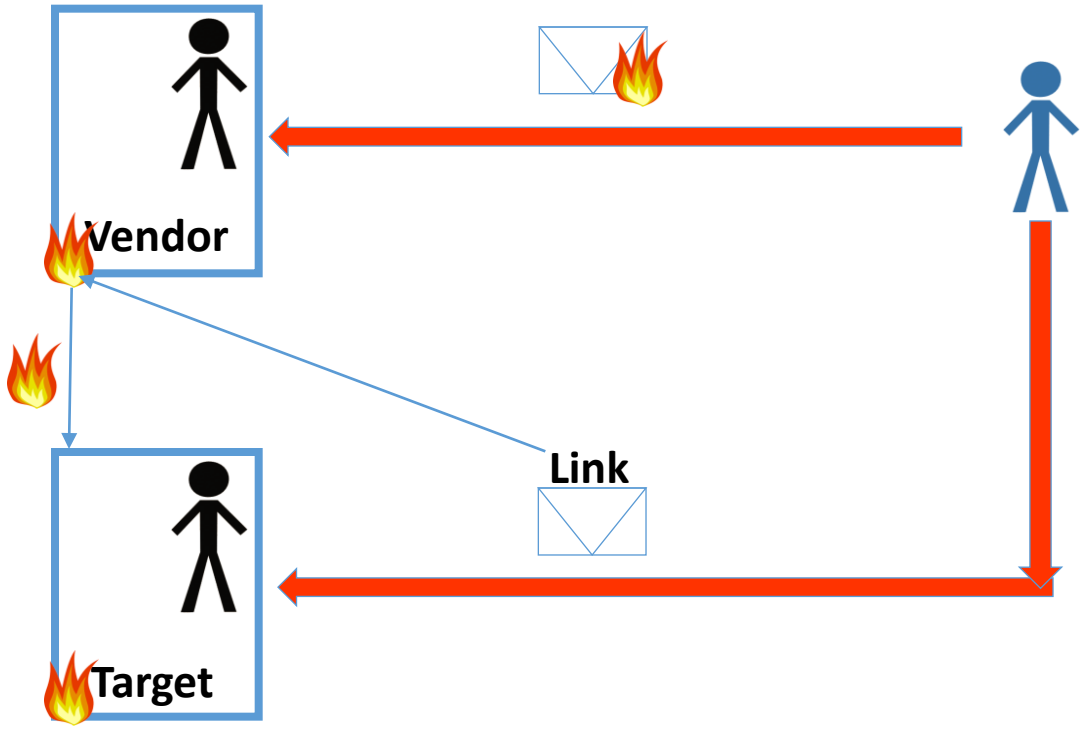
Combination attacks



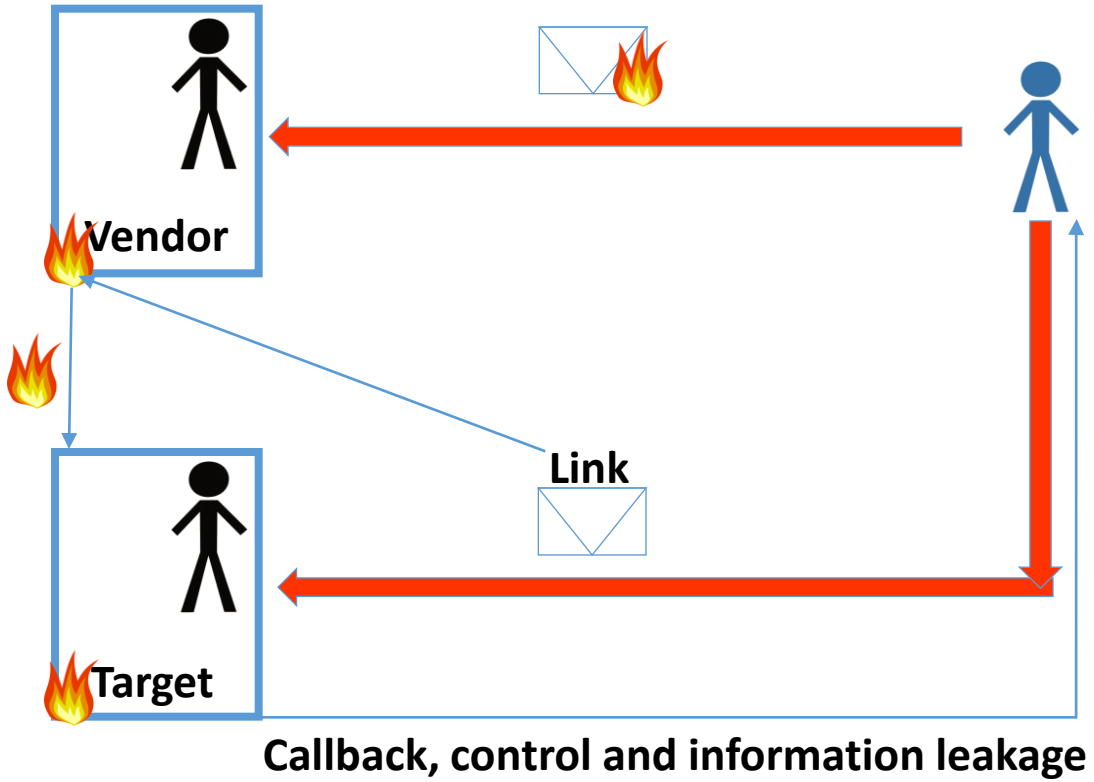
Combination attacks



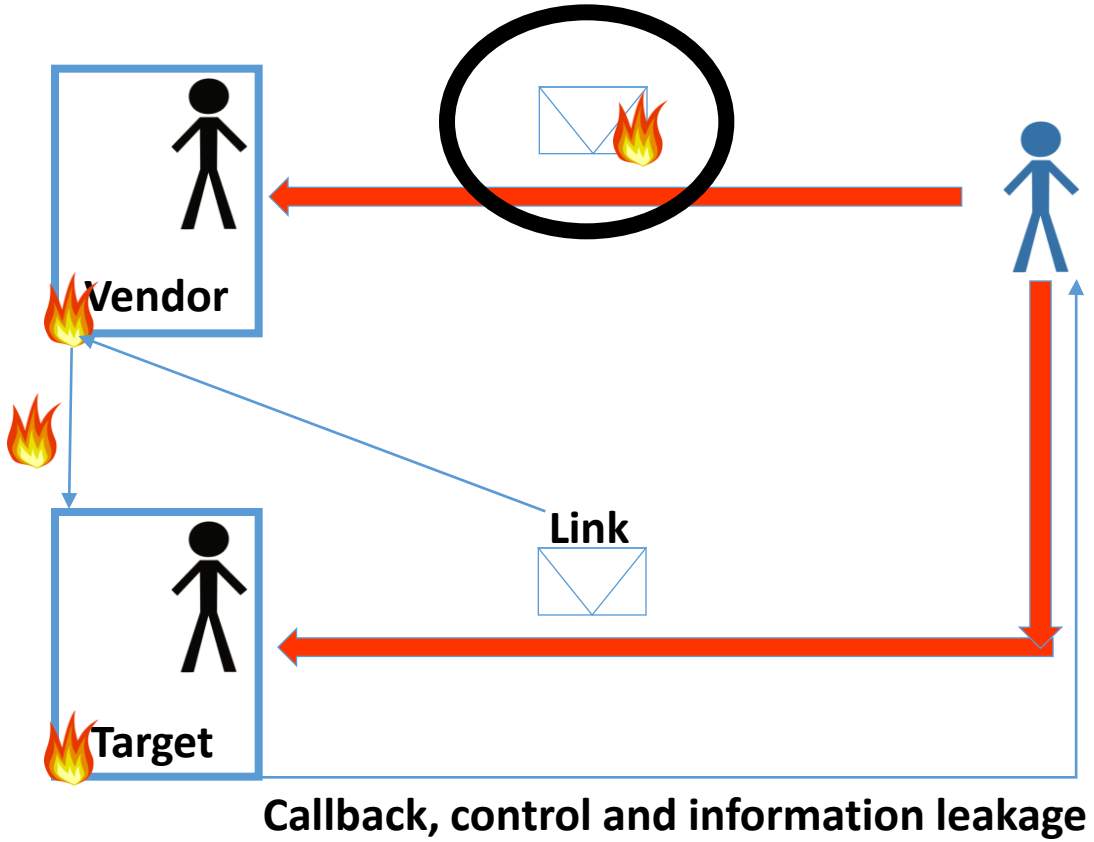
Combination attacks



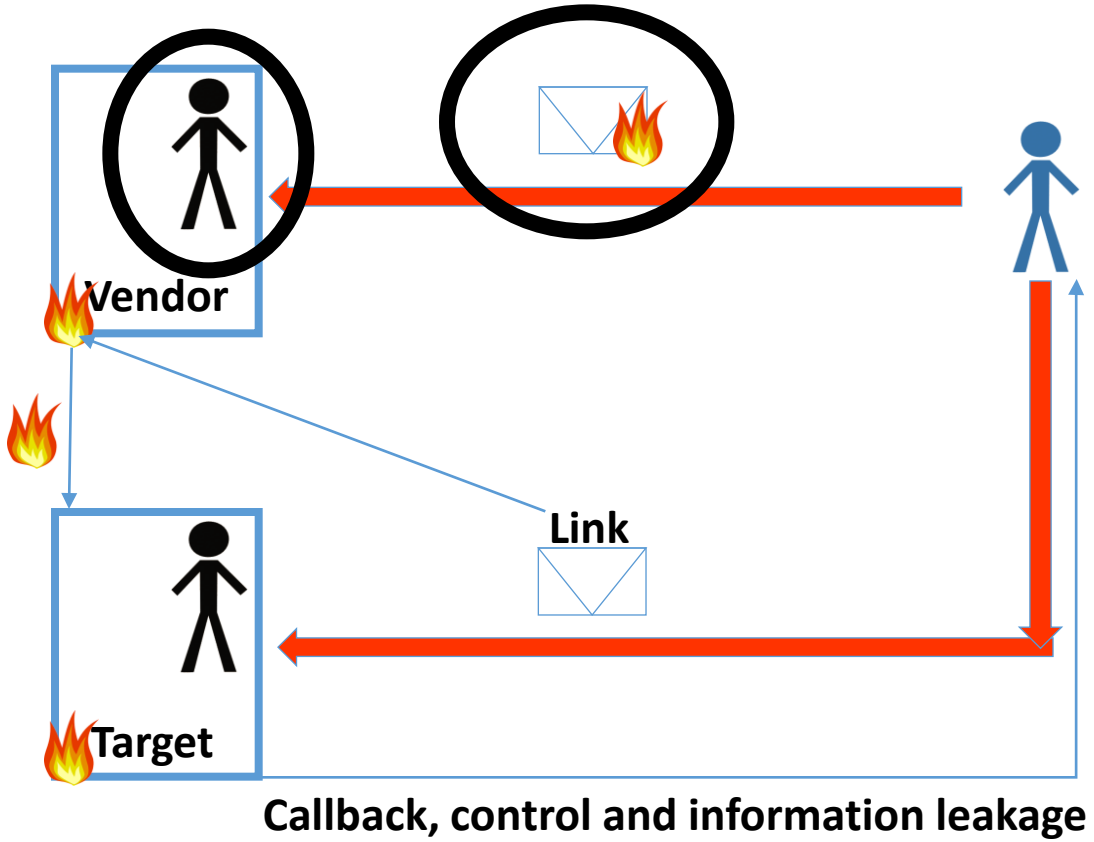
Combination attacks



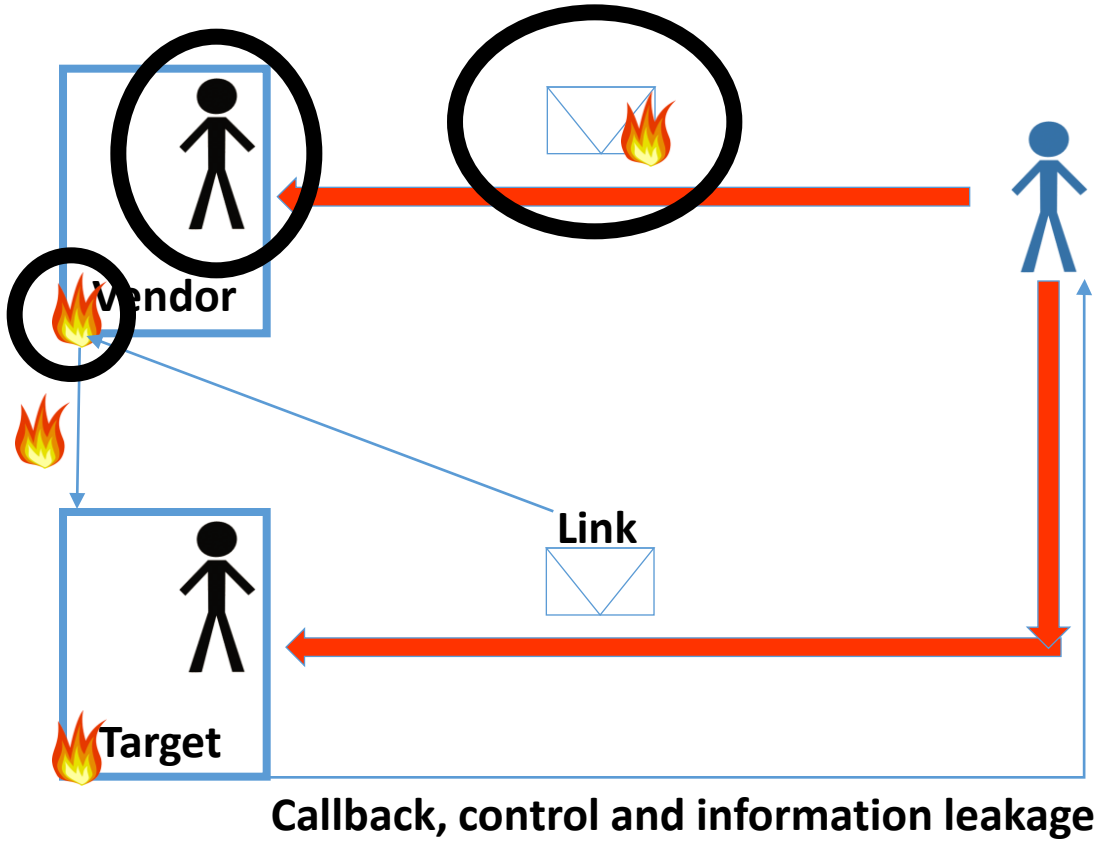
Detecting, assessing and reconstructing



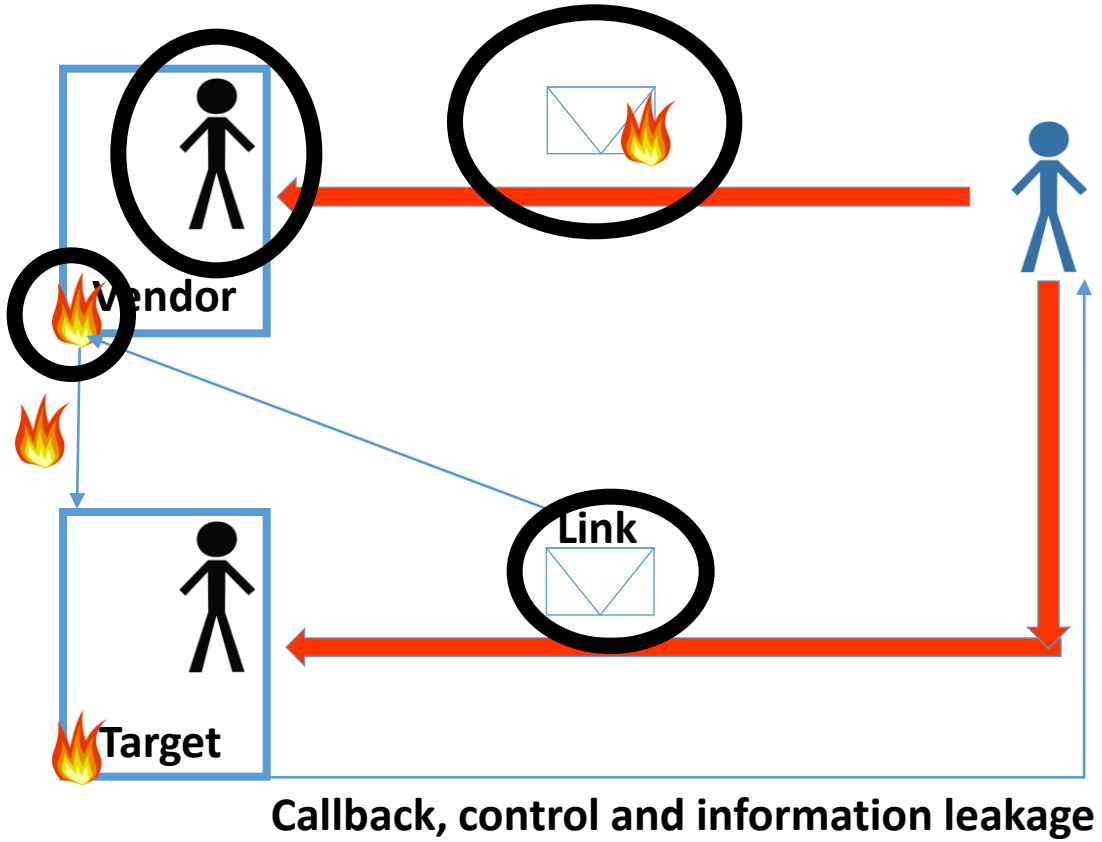
Detecting, assessing and reconstructing



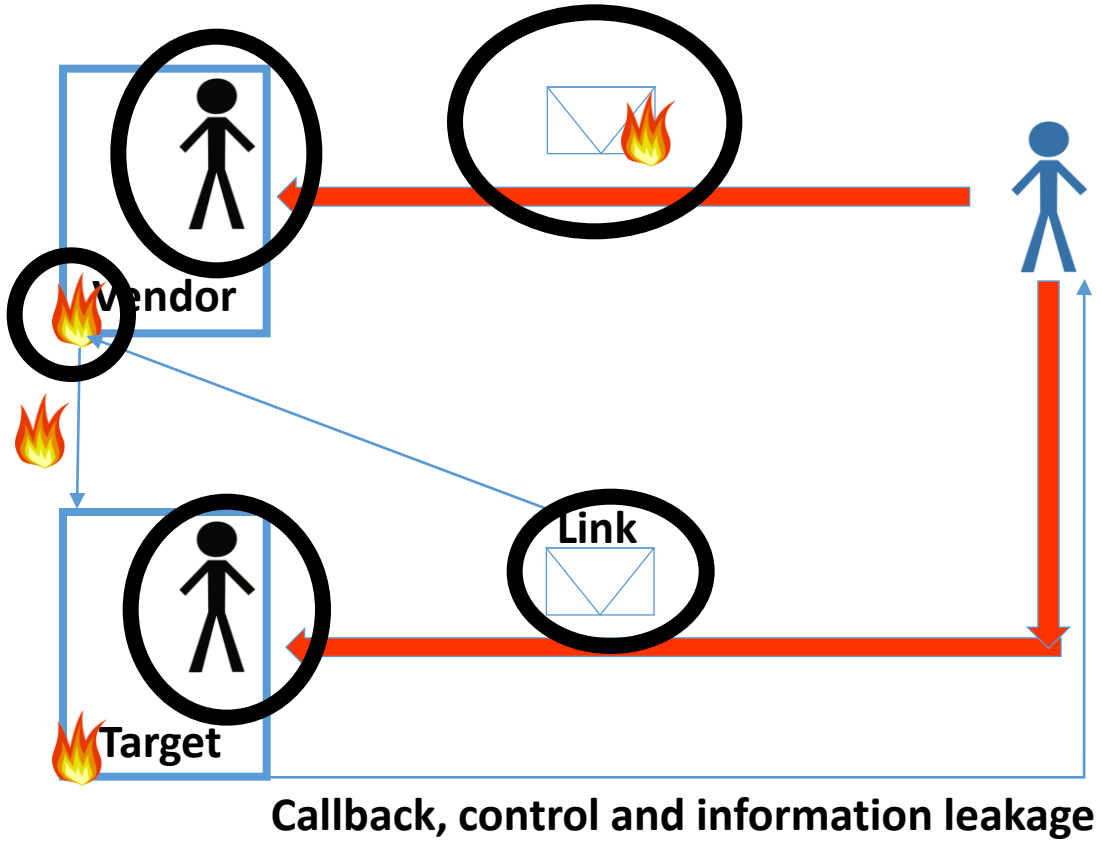
Detecting, assessing and reconstructing



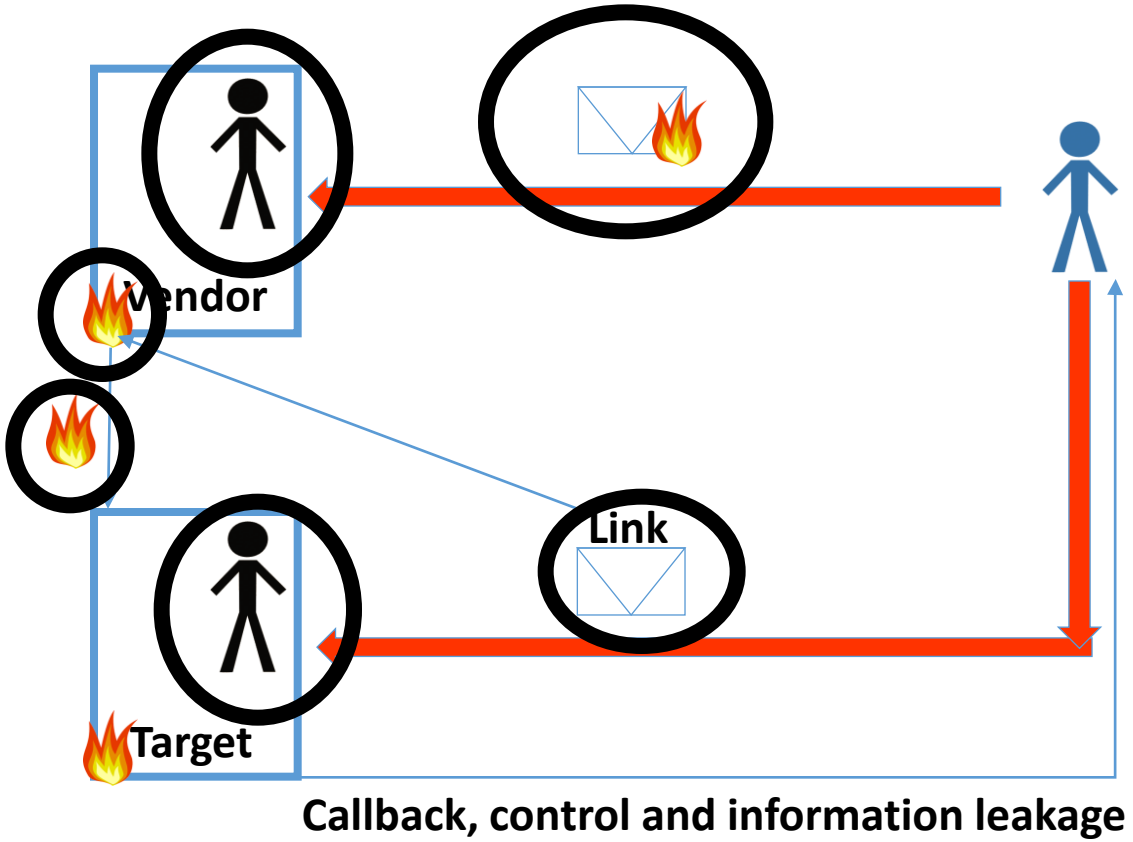
Detecting, assessing and reconstructing



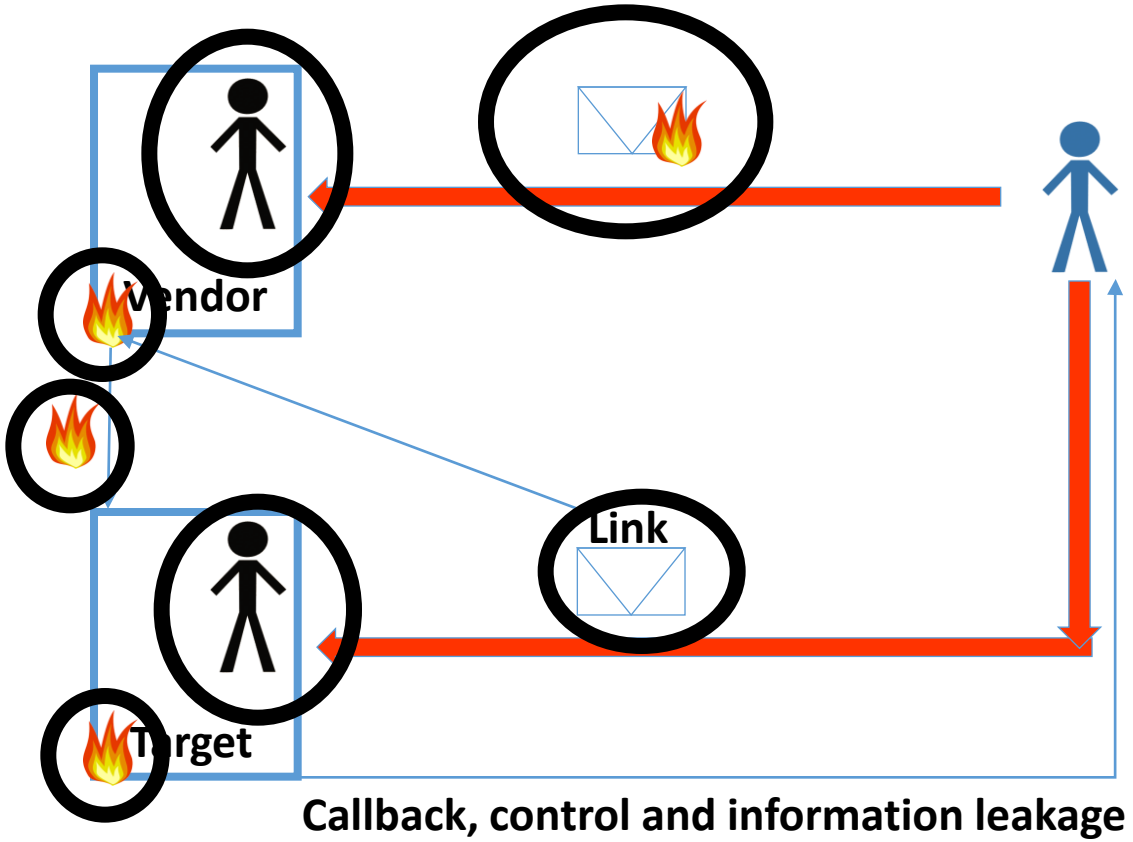
Detecting, assessing and reconstructing



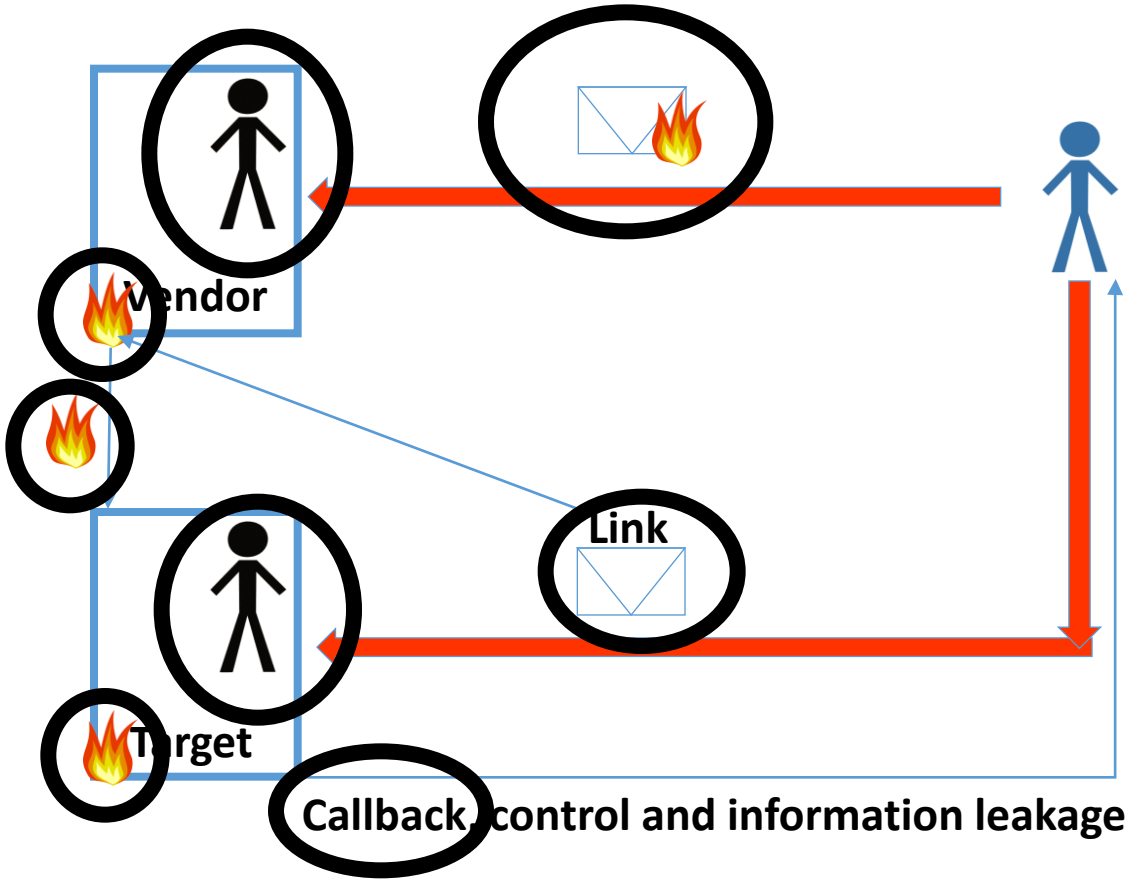
Detecting, assessing and reconstructing



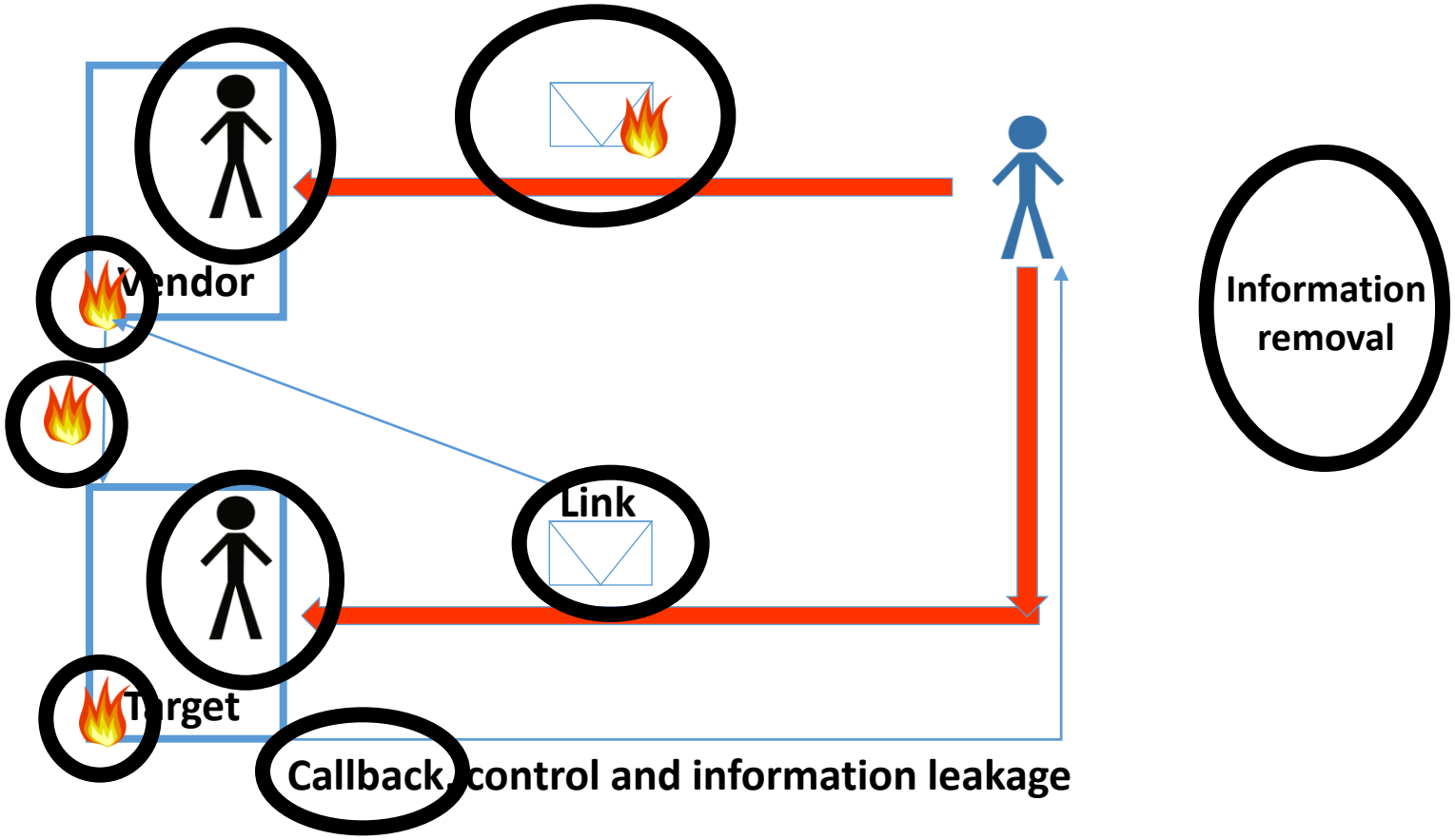
Detecting, assessing and reconstructing



Detecting, assessing and reconstructing



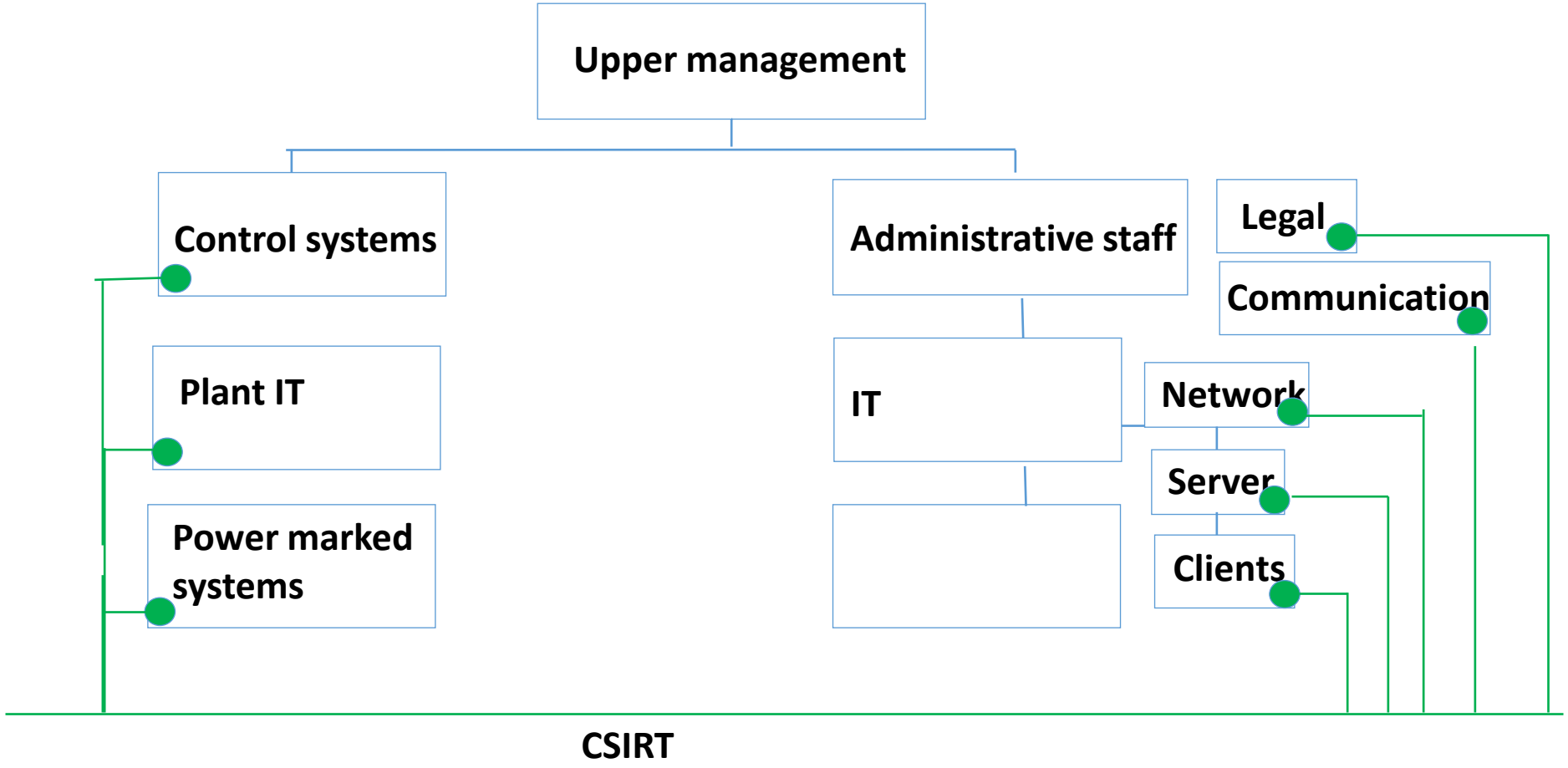
Detecting, assessing and reconstructing



Why a specialized incident response team?

- Incident handling is done faster and in a uniform manner
- Avoid costly mistakes
- The team knows what to do and whom to inform
- They regain control
- They reassure the organization AND the customers
- They can be an internal bridge between departments

Virtual team



CSIRT vs the emergency response team

- This team gathers at a certain severity level.
- The CSIRT starts earlier and work continuously together
- ERT deal with physical disasters and accidents
- Most CSIRTs deal only with information security incidents with an adversary (even if it is information leakage)
- The CSIRT must know when to call upon the ERT
- The ERT uses the IRT to assess damage, decide how to contain the incident, how to gather evidence etc.

FIRST.Org, Inc. All rights reserved.

The levels of severity need to be harmonized

- What the CSIRT calls a code red is not the same as for the ERT
- If the impact in production systems are unclear, all of the organization should be on alert, for example if a computer or a user that has access to the production network is hit by malware
- Again: the CSIRT should span all of the organization

FIRST.Org, Inc. All rights reserved.

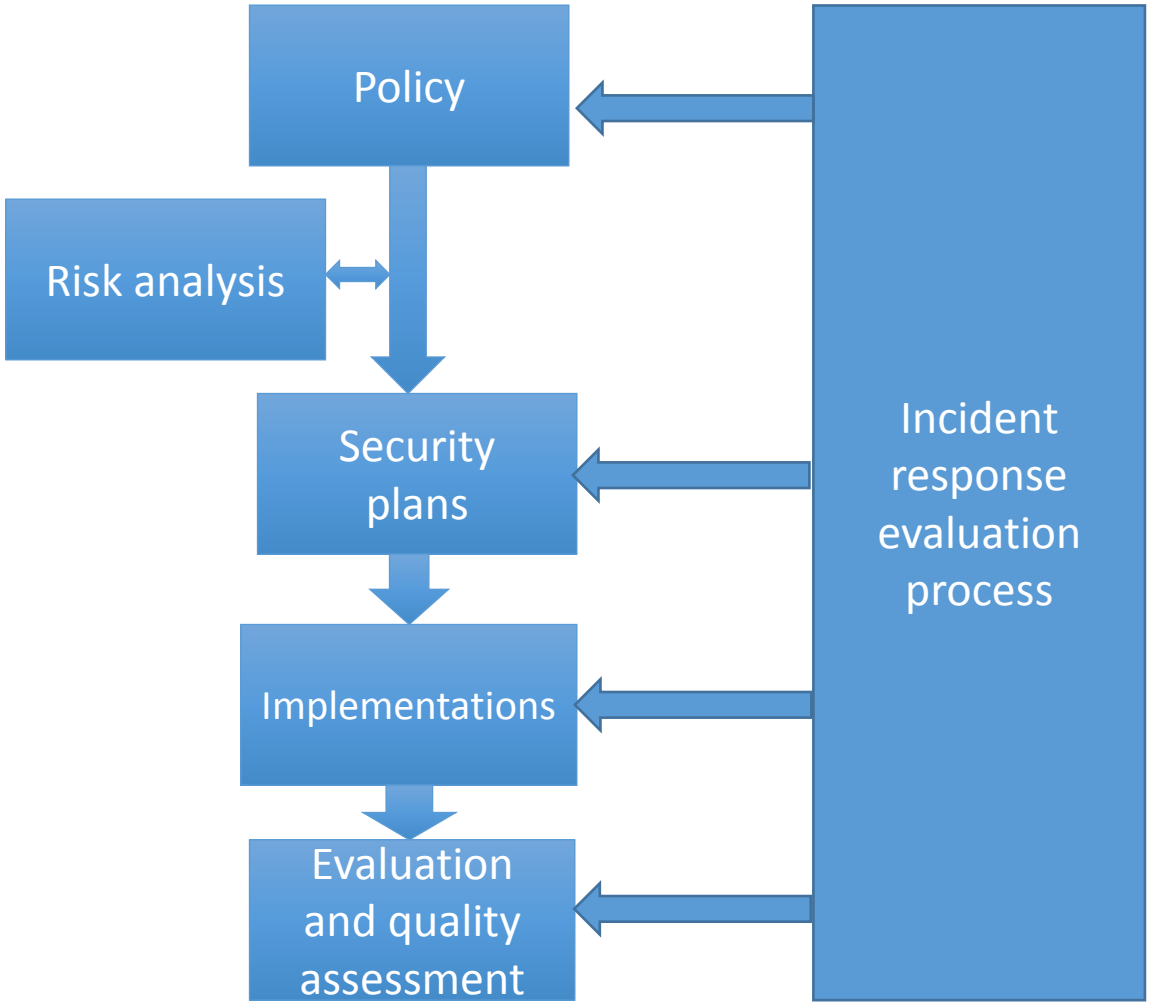
Working together

- The communication and setting the criticality should be exercised
- They should be aware of the other group's classification scheme
- The collaboration will evolve, and be dynamic
- They can be one team to rule it all, but you probably don't need the whole ERT in every meeting

FIRST.Org, Inc. All rights reserved.

Continuous improvement

- The feedback loop is crucial
- A CSIRT can improve the processes of
  - Policy making
  - Risk analysis
  - Security planning
  - Emergency planning
  - Evaluations & audits

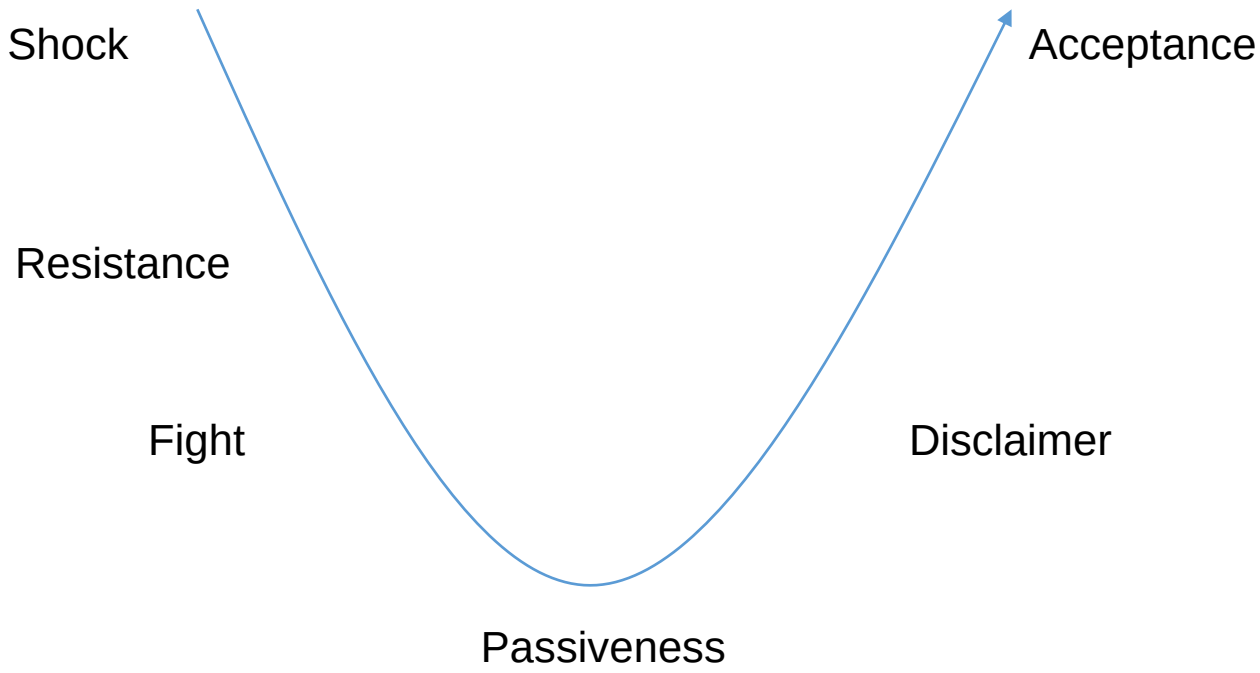


Reorganizing large organizations is like reorganizing a cemetery.

Organizational obstacles

- We have managed for years without!
- We *have* people doing security
- We have enough competence to cover this
- This will become a state within the state
- Will this just not cost us more money?

The stages of change



Organizational issues

Organizational issues

- Clear constituency

Organizational issues

- Clear constituency
- Mandate to manage and make changes

Organizational issues

- Clear constituency
- Mandate to manage and make changes
- Give the team time to develop culture

Who is your team?

Who is your team?

- The ones that log

Who is your team?

- The ones that log
- The ones that operate equipment that may be compromised

Who is your team?

- The ones that log
- The ones that operate equipment that may be compromised
- Communication

Who is your team?

- The ones that log
- The ones that operate equipment that may be compromised
- Communication
- Legal department

Who is your team?

- The ones that log
- The ones that operate equipment that may be compromised
- Communication
- Legal department
- People who are interested

They should be team players with

- Common sense
- Communication-and diplomatic skills
- Patience and persistence
- Creativity
- Serenity
- Discretion
- Concentration
- Tidy
- With technical skills and a good legal instinct

Incident detection

- Always difficult to identify an incident among false positives or from human error
- Even worse in control system: vague indicators, small changes, incomplete symptoms
- Baseline the system activity, the events and the traffic is useful, and of course log correlation with alarms.

The importance of tidiness

- Focus on ***what*** has happened
- Think of how you obtain evidence keeping the chain of custody
- Think of how you store evidence (sanitize and write lock)
- Digital signing and checksum
- Involve the legal department

Do I have SSL v.1.0.1? I don't knooooooooow…

Knowing your network

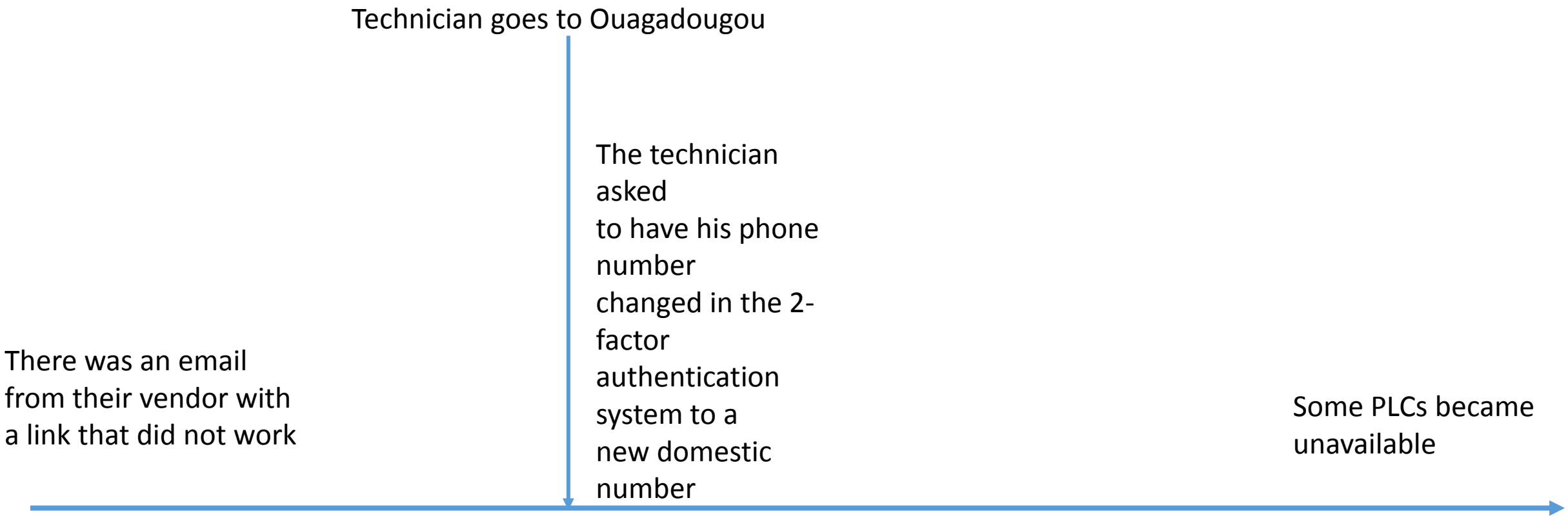
- It's too late to take inventory
- How does the information flow?
- What kind of information flows where?
- Knowing your protocols
- Knowing the best way to contain an incident (especially SCADA)
- Knowing the criticality of the resources

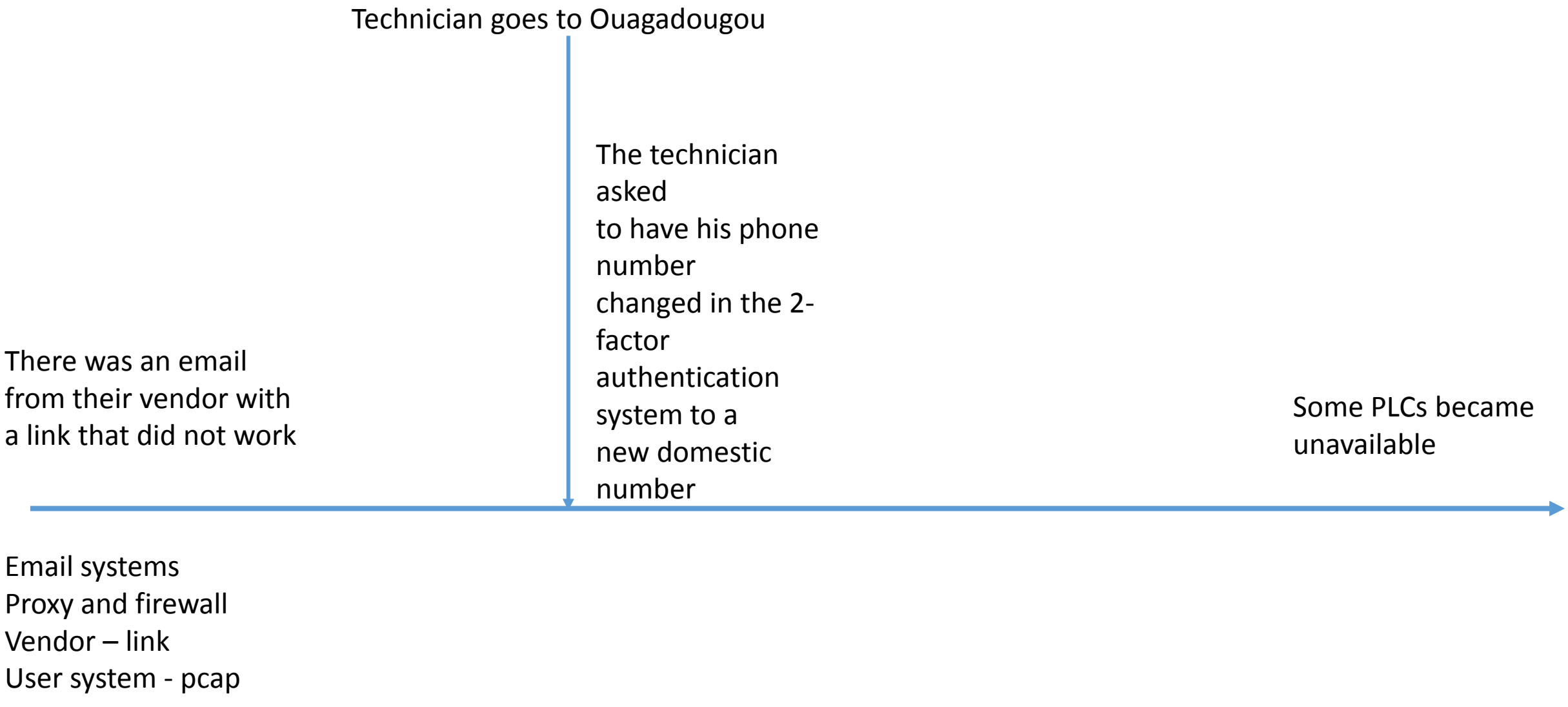
Knowing your logs

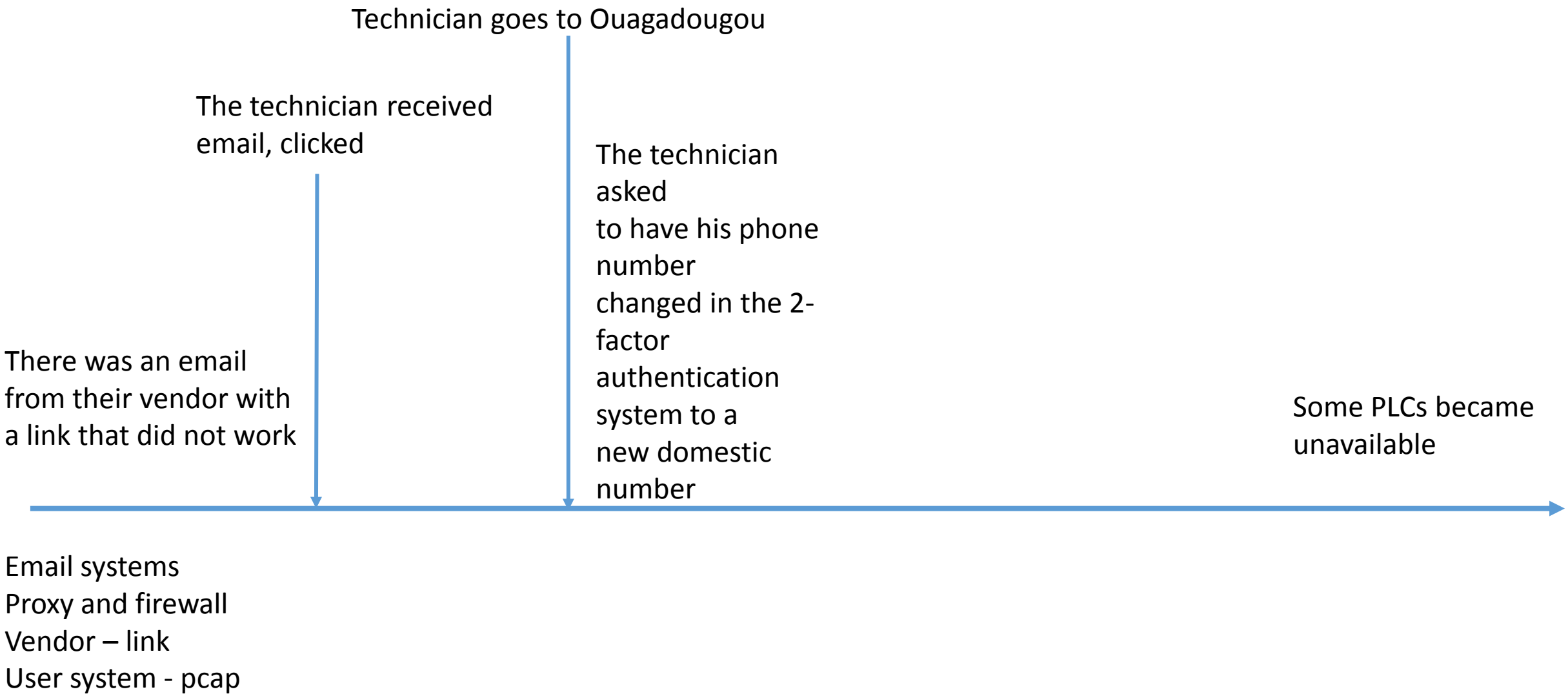
- Servers and user devices (including tablets and phones)
- ICS devices
- Network traffic (when the device does not log)
- Security appliances, VPN servers
- Directory services
- Name servers and DHCP-servers
- Web servers, proxy logs and application logs
- Databases
- Email and chat applications
- IP telephony logs
- Key cards, surveillance camera
- **Clocks and time format**

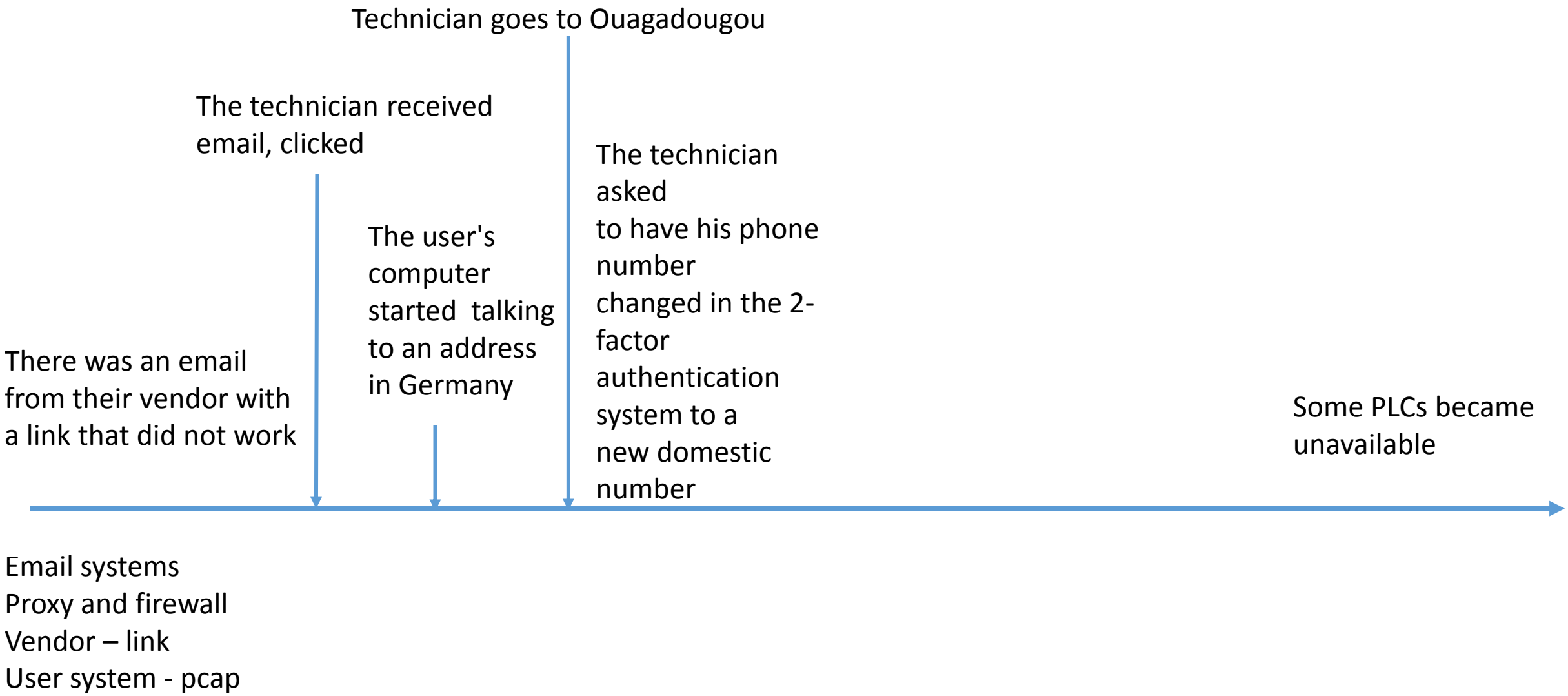
Establishing a timeline

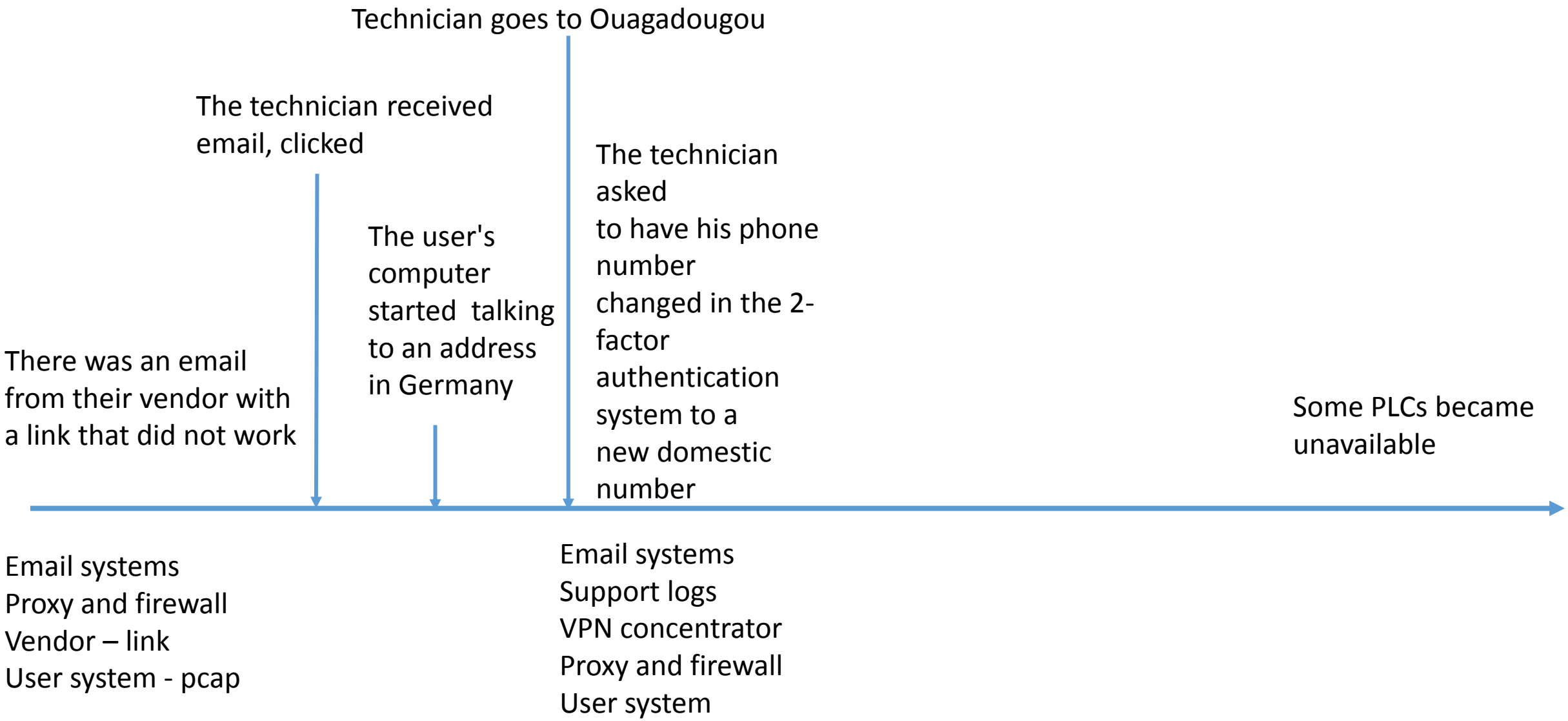
- Some PLCs became unavailable
- Technician is in Ouagadougou
- There was an email from their vendor with a link that did not work
- The technician asked to have his phone number changed in the 2-factor authentication system to a new domestic number

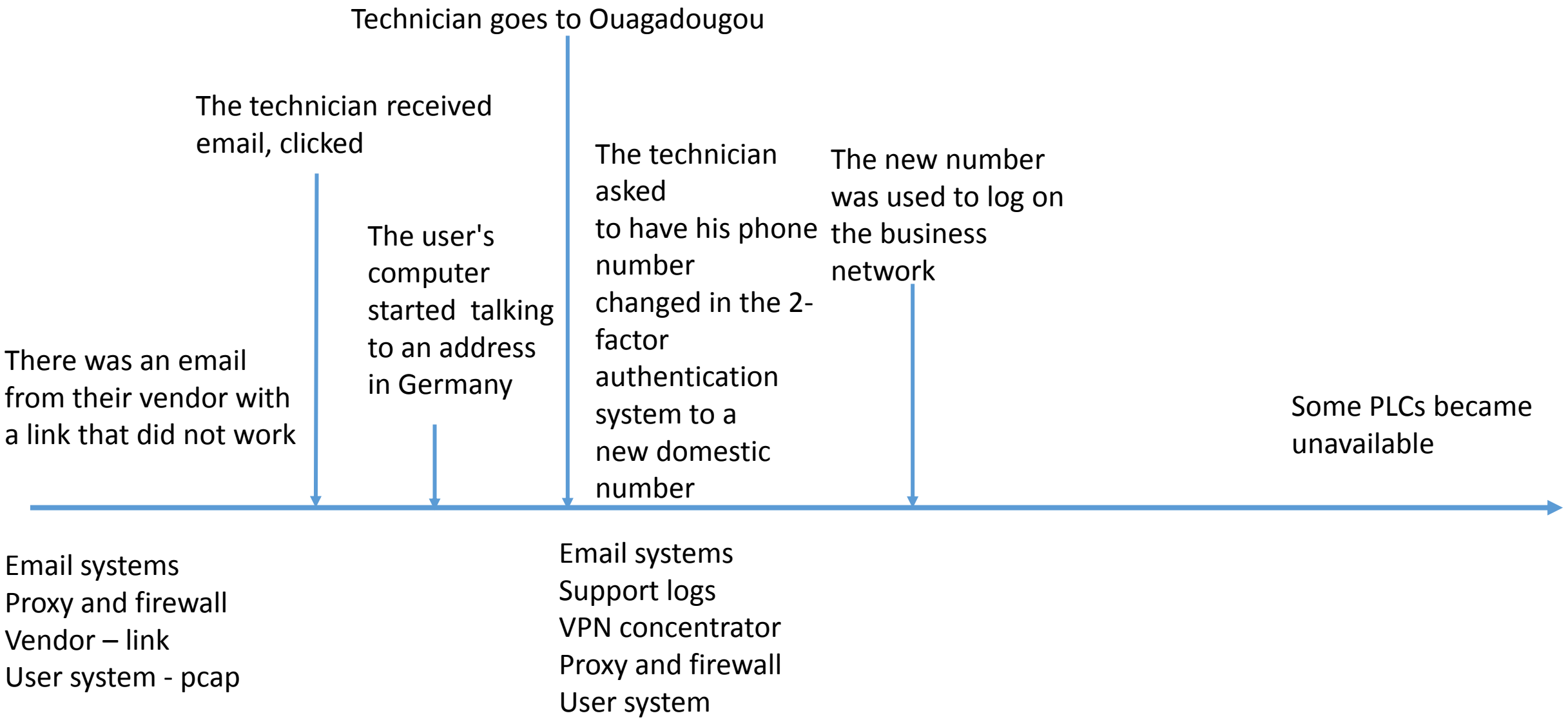

Technician goes to Ouagadougou
The technician asked to have his phone number changed in the 2-factor authentication system to a new domestic number
There was an email from their vendor with a link that did not work
Some PLCs became unavailable

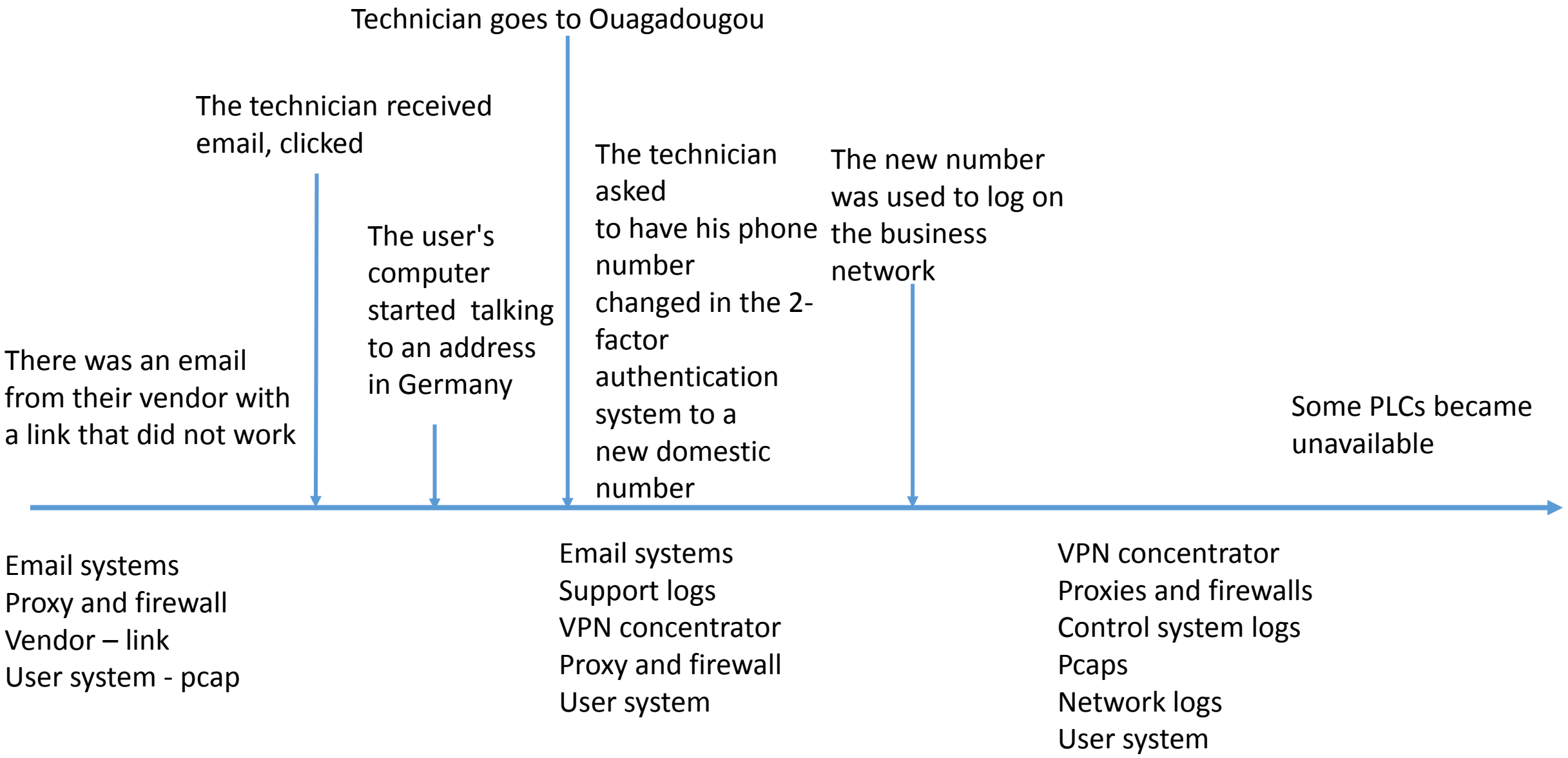

Technician goes to Ouagadougou
The technician asked to have his phone number changed in the 2-factor authentication system to a new domestic number
There was an email from their vendor with a link that did not work
Some PLCs became unavailable
Email systems
Proxy and firewall
Vendor – link
User system - pcap

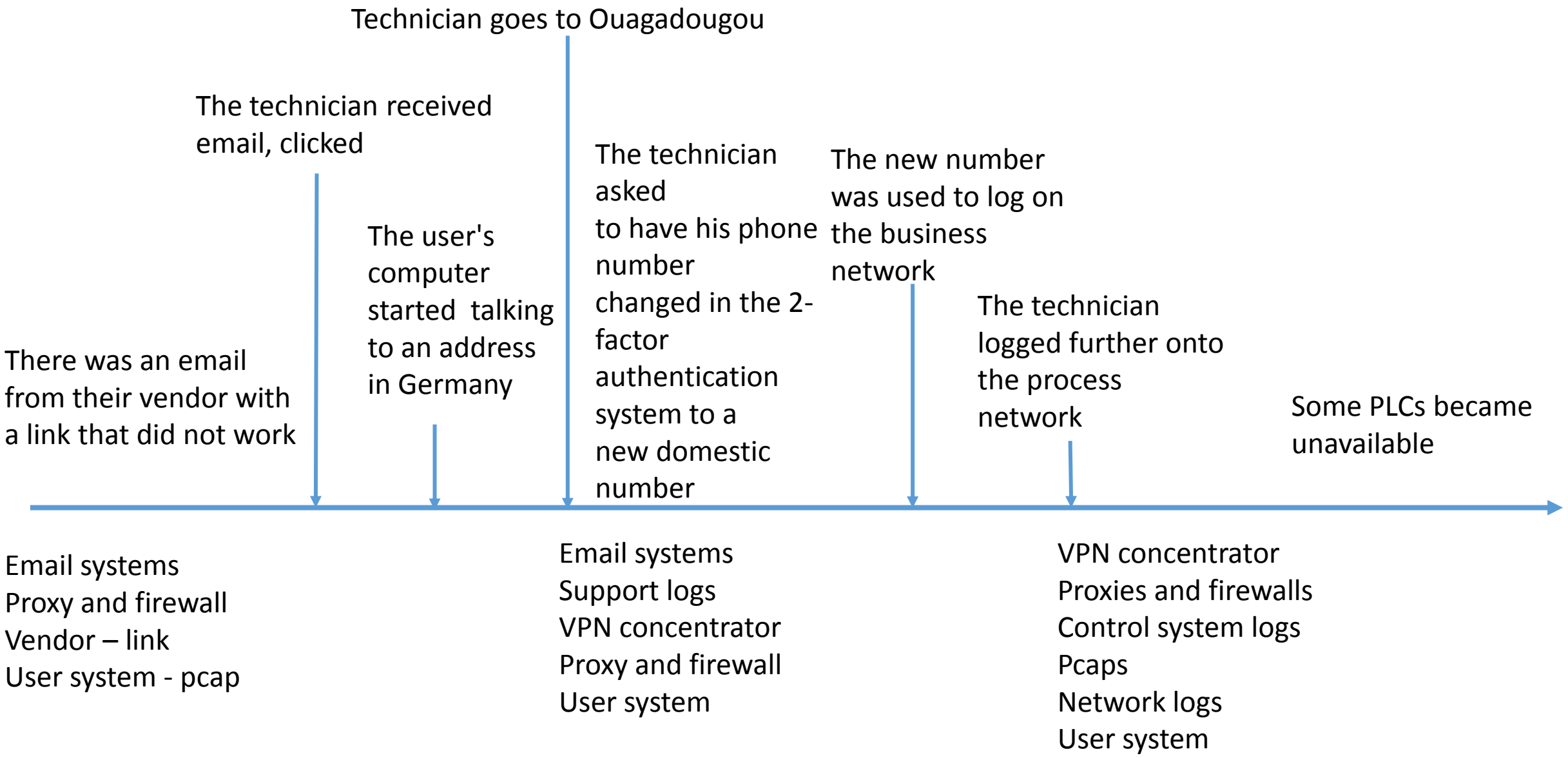

Technician goes to Ouagadougou
The technician received email, clicked
The technician asked to have his phone number changed in the 2-factor authentication system to a new domestic number
There was an email from their vendor with a link that did not work
Some PLCs became unavailable
Email systems
Proxy and firewall
Vendor – link
User system - pcap

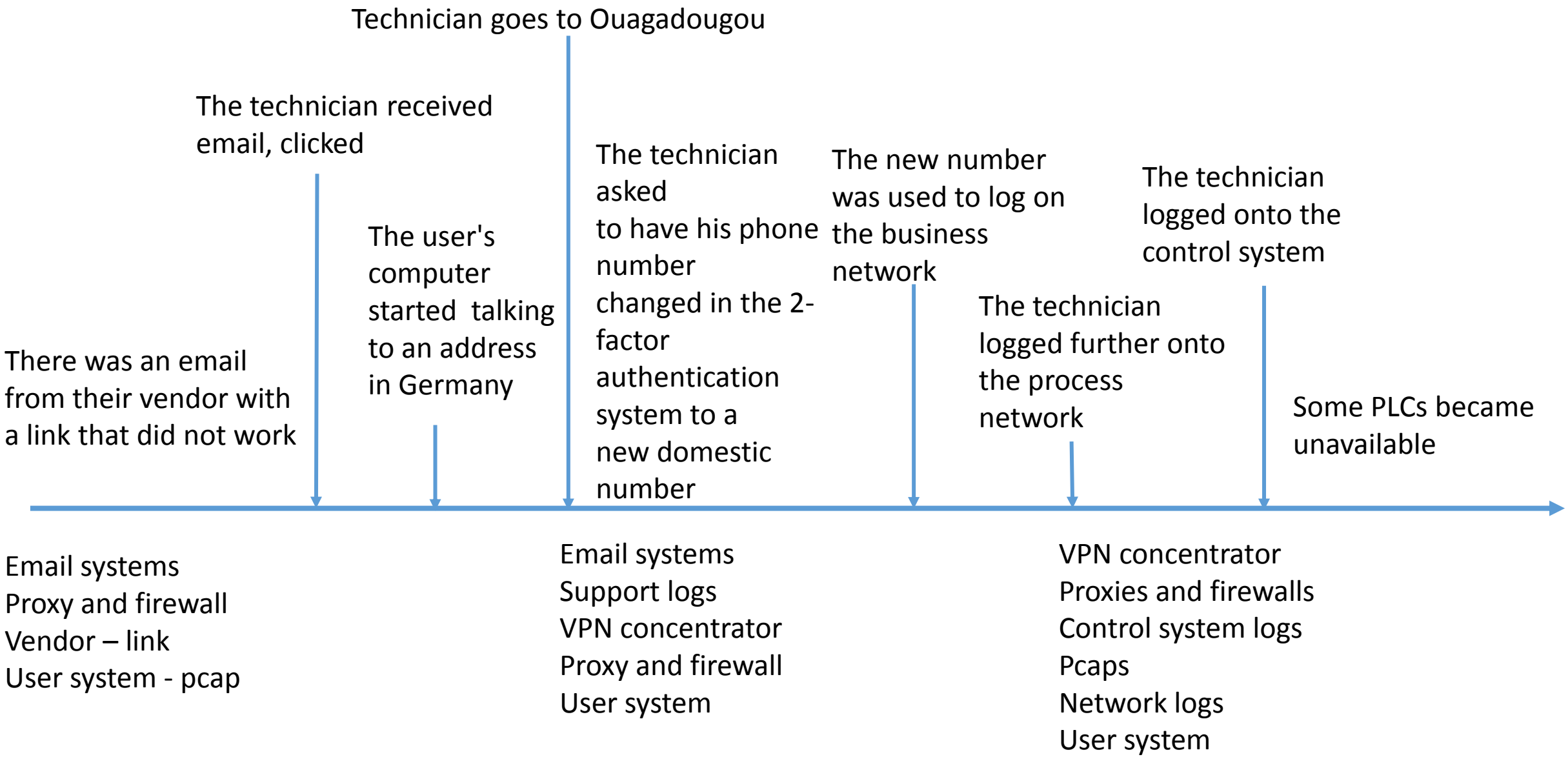

Technician goes to Ouagadougou
The technician received email, clicked
The user's computer started talking to an address in Germany
The technician asked to have his phone number changed in the 2-factor authentication system to a new domestic number
There was an email from their vendor with a link that did not work
Some PLCs became unavailable
Email systems
Proxy and firewall
Vendor – link
User system - pcap

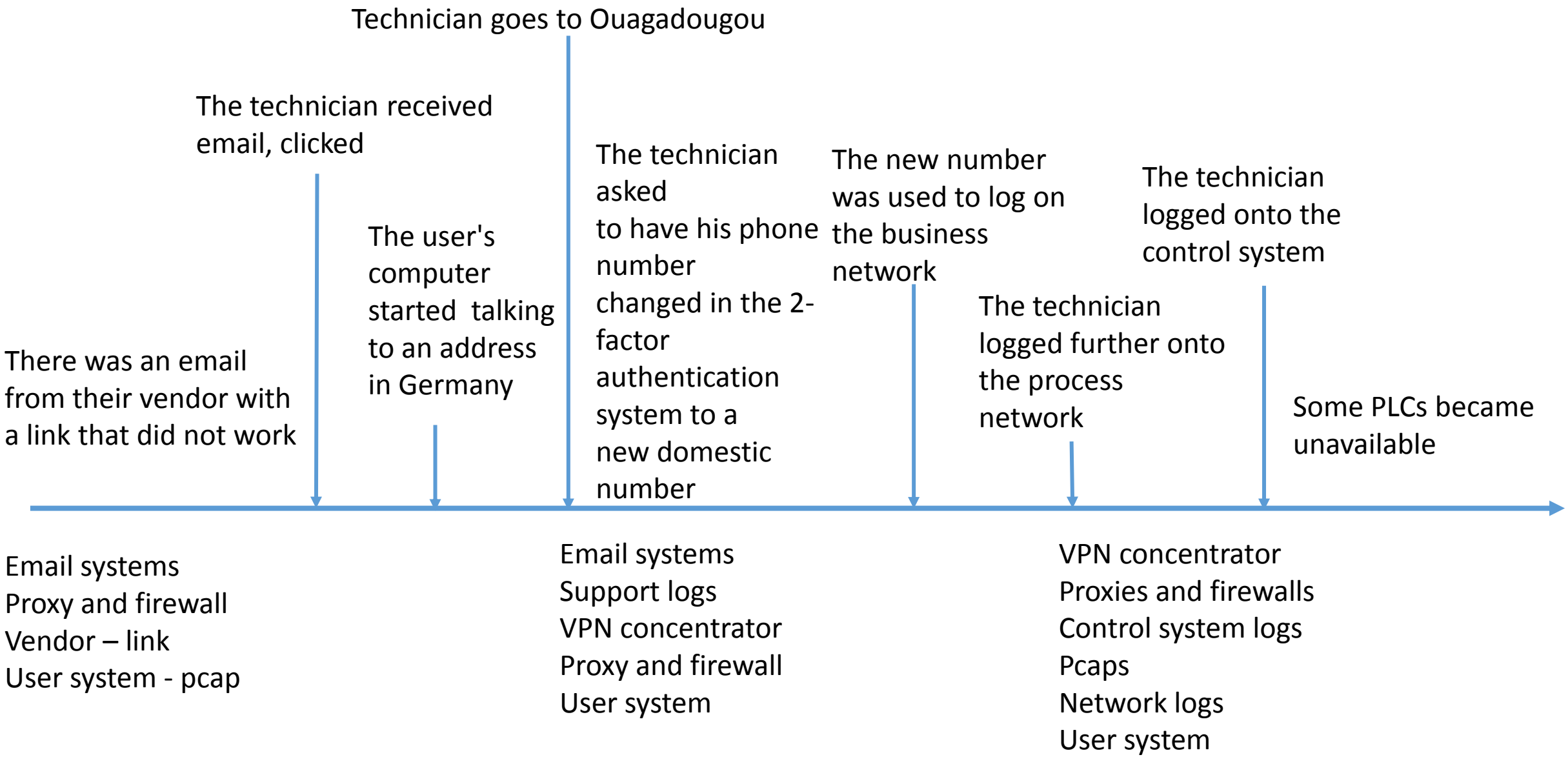

Technician goes to Ouagadougou
The technician received email, clicked
The user's computer started talking to an address in Germany
The technician asked to have his phone number changed in the 2-factor authentication system to a new domestic number
There was an email from their vendor with a link that did not work
Some PLCs became unavailable
Email systems
Proxy and firewall
Vendor – link
User system - pcap
Email systems
Support logs
VPN concentrator
Proxy and firewall
User system


Technician goes to Ouagadougou
The technician received email, clicked
The user's computer started talking to an address in Germany
The technician asked to have his phone number changed in the 2-factor authentication system to a new domestic number
The new number was used to log on the business network
There was an email from their vendor with a link that did not work
Some PLCs became unavailable
Email systems
Proxy and firewall
Vendor – link
User system - pcap
Email systems
Support logs
VPN concentrator
Proxy and firewall
User system


Technician goes to Ouagadougou
The technician received email, clicked
The user's computer started talking to an address in Germany
The technician asked to have his phone number changed in the 2-factor authentication system to a new domestic number
The new number was used to log on the business network
There was an email from their vendor with a link that did not work
Some PLCs became unavailable
Email systems
Proxy and firewall
Vendor – link
User system - pcap
Email systems
Support logs
VPN concentrator
Proxy and firewall
User system
VPN concentrator
Proxies and firewalls
Control system logs
Pcaps
Network logs
User system


Technician goes to Ouagadougou
The technician received email, clicked
The user's computer started talking to an address in Germany
The technician asked to have his phone number changed in the 2-factor authentication system to a new domestic number
The new number was used to log on the business network
The technician logged further onto the process network
Some PLCs became unavailable
There was an email from their vendor with a link that did not work
Email systems
Proxy and firewall
Vendor – link
User system - pcap
Email systems
Support logs
VPN concentrator
Proxy and firewall
User system
VPN concentrator
Proxies and firewalls
Control system logs
Pcaps
Network logs
User system


There was an email from their vendor with a link that did not work
The technician received email, clicked
The user's computer started talking to an address in Germany
Technician goes to Ouagadougou
The technician asked to have his phone number changed in the 2-factor authentication system to a new domestic number
The new number was used to log on the business network
The technician logged further onto the process network
The technician logged onto the control system
Some PLCs became unavailable
Email systems
Proxy and firewall
Vendor – link
User system - pcap
Email systems
Support logs
VPN concentrator
Proxy and firewall
User system
VPN concentrator
Proxies and firewalls
Control system logs
Pcaps
Network logs
User system



Evidence:
Statements, logs, pcap, forensic images from user, vendor and possibly control system

The answer should be "yes" to these questions

- Can you fire up packet capture?
  - Corollary: do you have active taps, span ports or a hub?
  - In the process network?
- Can you do a forensic image?
  - Corollary: do you have somewhere to store it?
- Can you capture volatile data?
- USB forensic tools ready

Information plans

- To keep people happy
- To build trust
- To leave the team working uninterrupted
- To create predictability and standards
- Do not release info too soon. It may be plain wrong.

Information list

- Systems owner
- Several levels of management
- Emergency team/disaster recovery/business continuity
- Legal department
- Communications
- Regulatory authority
- The public

Being lazy

Automation

- If you're going to do this again, you need to automate
- If you can't find somebody who can
- If you can't find anybody, team up with someone else

I need HELP!

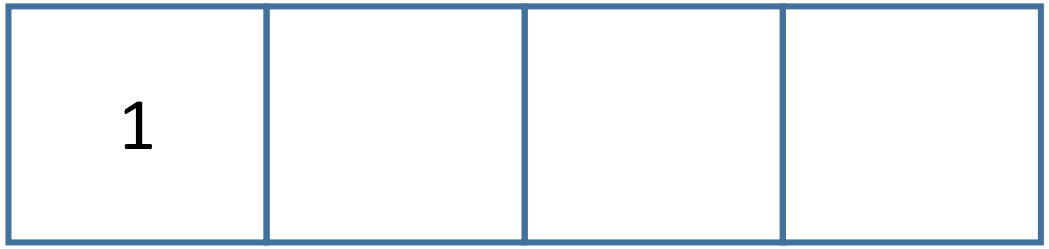
- Forensics analysis
- Reverse engineering
- Behavioral analysis
- Identifying the attacker
- Recovery is often not done by the CSIRT

The important process of lessons learned

- When you know how it happened, you know how to prevent it
- This can be powerful knowledge to share with other teams
- The measures should be part pf the lessons learned


Incident

- If the report is put in a drawer or otherwise hidden, you are back at:



Collaboration and sharing

- Some attacks happen sector wise (and technology wise)
- Some attacks happen country wise
- Attack patterns follow certain trends
- We should link up for relevant early warning and for learning purposes
- Ideally we should learn from other people's lessons as well as our own

- Questions?
- I can also be reached at margrete.raaum@statnett.no or margrete.raaum@first.org