To be unprepared

A Thursday at the District heating plant.

Why can’t I load the device drivers? What do I do now?
Oh no, we will have trouble delivering heating if we can’t solve this. What is going to happen? What should we do?
I am sorry that we have to call you! It’s complete chaos around here. No-one knows how to restore the system and we can’t find anything in the manual.
The heat production is finally restored.

What a day! So much time, money and energy spent! Everyone is exhausted.
Recommendations

• Maintain processes for system surveys and risk management in industrial information and control systems.
  – There should be a clear and updated documentation on the operation’s systems, information flows and system dependencies.
• Conduct training and practice regarding IT incidents in industrial information and control systems.
• Ensure systematic contingency planning and incident management in industrial information and control systems.
Ensure that the following items are included in the contingency planning:

- routines for handling operations manually (run the process without computer support).
- routines for restoring both data and configuration settings as well as restarting the process.
- contact details for system owners, operators, service technicians, other personnel, vendors and support.
- description of support agreements and suspension times.
- description of how central control system components can be replaced.
- description of how and from where emergency operations are to be conducted if the disturbance is serious.
To be proactive

Look what’s happened in the neighbouring municipality! How can we make sure this doesn’t happen to us?
We have received more information. We have to prioritise this risk and act accordingly.
Let’s make some changes to the network architecture.

A firewall between the production and administration is installed.
Everything looks good. It is all in line with the decisions made in our risk analysis. We are continuously monitoring all network communications.
Recommendations

- Follow up incidents in industrial information and control systems and monitor external security problems.
- Conduct regular risk analyses of industrial information and control systems.
- Work with a security architecture in the industrial information and control systems.
- Maintain processes for system surveys and risk management in industrial information and control systems.
- Participate in user associations, standardisation bodies and other networks for security in industrial information and control systems.
Protect vital societal functions.
Protect your organisation.
Protect your industrial control systems.