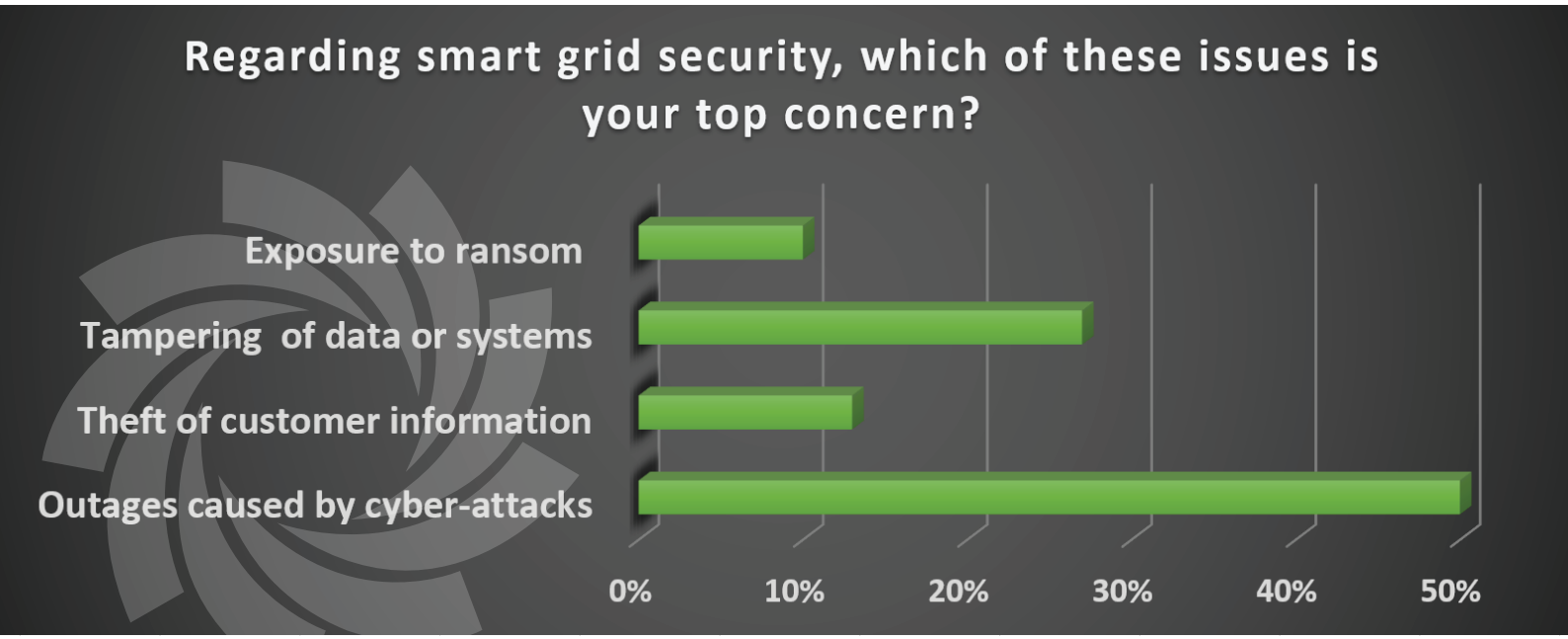
CYBER-SECURITY CONCERNS, SURVEY RESULTS 2021

OSGP Alliance presents the outcome of a survey on the top concerns for cyber-attack on the smart grid - released in May 2021.



Cyber-security of the smart grid is an increasing concern for DSOs. Before the smart grid became smart, the cyber-criminals had no means of attacking it. Smarter grids improve automation, monitoring, management and maintenance of the energy grid, to reduce fraud and theft, reduce energy losses, introduce green and locally produced energy and increase sustainability. The technology enabling allows cyber-criminals to damage this critical energy transformation.

Cyber-attack causes several outcomes:

- Outages caused by cyberattack, **50%** in our survey - a cyber-attack results in denying access to energy through turning the supply off or damaging the smart grid.
- Theft of customer information, **13%** in our survey - a cyber-attack results in the customers' energy usage information being exposed.
- Tampering of data or systems, **27%** in our survey - a cyber-attack results in billing, usage, operational and energy quality information being maliciously corrupted, impacting the DSOs' ability to bill and operate the grid efficiency, safely and reliability.
- Exposure to ransom, **10%** in our survey - a cyber-attack, potentially covering any of the three cases above, is used as the basis for ransom – the DSO needs to pay the attacker to avoid suffering the consequences.

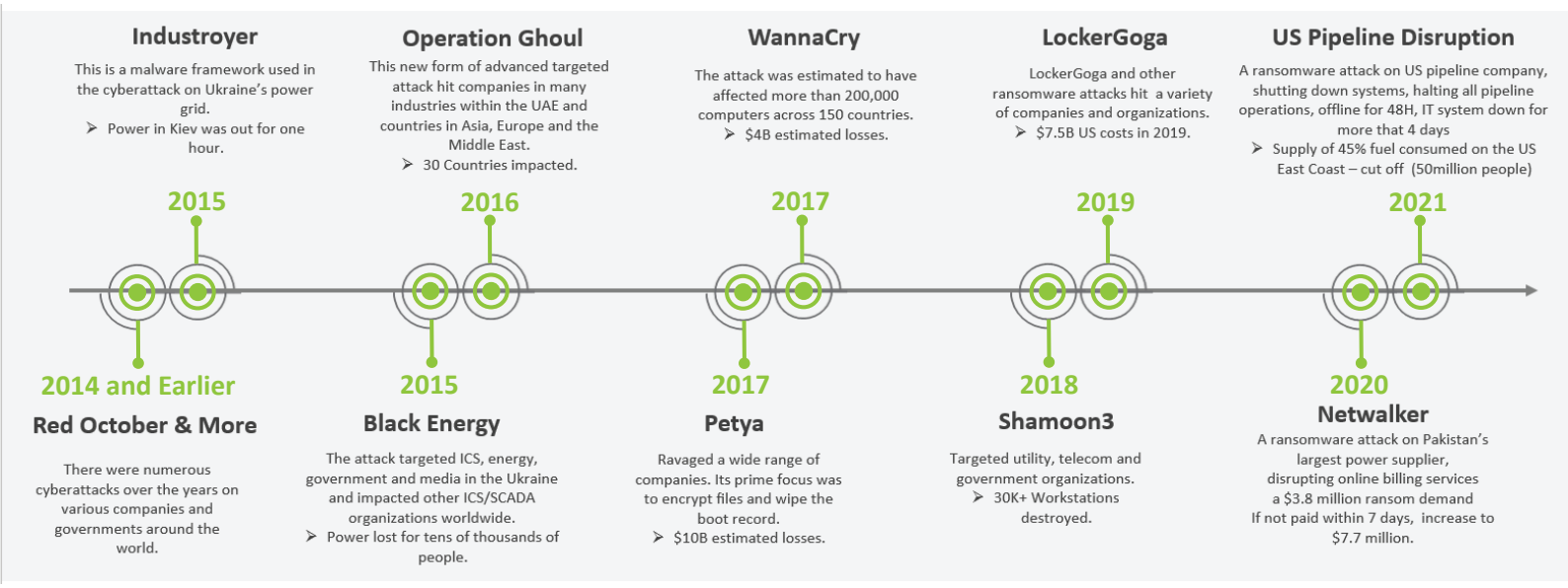
Based on this survey, **concerns of outages** are by far the most significant issue; energy infrastructure is a critical resource, and denial of access to energy, even for a few hours, can have significant consequences. It is not just about convenience – it is also about health and safety and efficiency of businesses relying on the energy supply. Reliability is becoming a regulatory requirement for DSOs with SAIDI and SAIFI (System Average Interruption Duration/Frequency Index) becoming regulated KPIs. This, in addition to the reputational damage suffered by a DSO due to outages, is cause for concern.

Second place is the **tampering of data or systems**. If we focus on the billing information, the issue here is about fairness of supply to all. If cyber-criminals can subvert the billing activities, the DSO is damaged, and the consequence is often to compensate through increased prices for all. Just like in insurance fraud, far from being a victimless crime, it is everybody that pays the cost. Tampering with operational and service quality information damages the overall efficiency in our energy supply and can result in increased energy wastage.

It is interesting that **exposure to ransom** is still low. This is the typical outcome of an attack by organised crime. It is often the hostile nation state or terrorist motivated attacks which aim at outage and have the resources to do so. Recently, there has been a significant up-surge in attacks motivated by financial gain through ransom demands, some of which have resulted in energy availability or increased cost to the consumer.

This is why the leading smart meter providers focus their energy on cyber-security protection. But, is protection enough? In your home, you rely on locks (protection), but many will purchase security lighting and burglar alarms (threat detection and response). OSGP Alliance Members are investing in sophisticated solutions for threat detection and response for their smart meters; augmenting already industry leading protection measures to increase the security of the smart grid.

SECURITY THREATS CONTINUE TO INCREASE



Sources: 1 – ISC2's Cyberthreat Defense Report 2020 2 – Indegy's Cyber Attacks on Critical Infrastructure – A Historical Timeline

The OSGP offers unique capabilities to make this possible.

- First, **security is "always on"** – there is no option for mistakes in configuration to expose weaknesses and no way for the attacker to turn security off as part of their exploitation.

- Second, OSGP offers a number of **unique features in its communications** protocols which offer enriched indicators of threat and suspicious activity, making it harder for the cyber-criminal or hostile nation state to establish a beachhead from which to launch an attack.

With OSGP and OSGP Alliance Members you get the smart grid equivalent to a burglar alarm that you can't forget to turn-on, the attacker can't disable, and which offers more tripwires and sensors than the attacker can cope with. That is not just a defensive system; it is a viable and credible deterrent.

Authors:

OSGP Security Workgroup

The OSGP Alliance has released this survey results in a joint cooperation between the OSGP Alliance and its members.

Contact: info@osgp.org

OSGP ALLIANCE

www.osgp.org