THE NATIONAL CYBERSECURITY SOCIETY

Tolerable Level of Loss

What is the Tolerable Level of Loss and how do I calculate it for my business?

Managing risk is a balancing act for organizations of all sizes and disciplines. While some organizations and businesses take on too much risk, others arguably do not take on enough. Because the consequences of cybersecurity failures can be damaging to your business revenue and brand reputation, it is important that you assess your tolerable level of loss and implement measures to mitigate the risk of losing your organization's most critical assets.

Tolerable level of loss is defined as a numeric value identified through a cost-benefit analysis that represents the **tolerable level** of material injury or loss from a cybersecurity event. A quick way to think about this is to determine what is the maximum ransom your business would pay a hacker to retrieve your data or systems from ransom.

FACT 1: Analysis

To assess your tolerable level of loss, there are four key questions to consider:

1. What losses would be catastrophic?
2. What can we live without, and for how long?
3. What information absolutely cannot fall into the wrong hands or be made public?
4. What could cause personal harm to employees, customers, partners, and visitors?

Leverage your team to talk through each of the questions above, and categorize assets according to people, technology, and intellectual property. If possible, try to measure the potential cybersecurity loss relevant to each critical asset in monetary units. Hard currency costs may include fines, legal fees, lost productivity and mitigation, remediation, and incident response, as well as the cost to recreate or rebuild the asset that was lost.

Did you know?

- √ Ransom attacks are continuing to increase in sophistication and price of bounty
- √ You have fire insurance, why not cyber insurance?
- √ See our cyber insurance resources and ask for a quote

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service, **web@thencss.org** or visit us at the link below.

Tolerable Level of Loss continued....

Other costs are more difficult to quantify – they are qualitative and long lasting. These include diminished brand equity, reduced goodwill, and the loss of intellectual property, all leading to weaker market position, or, in some cases, complete elimination of competitive advantage.

Once you have discussed and calculated, to the best of your ability, the value of each asset, prioritize your assets. A good first step is identifying and classifying applications, databases, systems, and information. A practical classifications scheme (in descending order of importance) is presented below:

1. Mission and Business Critical Systems. In aggregate, these are the vital elements of the business where the most sensitive information resides. Include intellectual property, information and physical assets, and systems required to run the business. This includes information that can also impact life or death.
2. Core Infrastructure, Extended Ecosystem. Common examples include customer relationship management applications and partner portals.
3. External, public-facing systems and points of interaction. Common examples include web servers and systems with IP addresses accessible through the internet.

Your tolerable level of loss will be based upon the quantitative and qualitative value of your prioritized assets and your projected ability to sustain your organization in a catastrophe. Once derived, this value can be used to quantify your cyber insurance policy. See our resources under Cyber Insurance/Member Perks.

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.