MAINTAINING BUSINESS CONTINUITY

The world of gaming has never been more interesting than it is today, with cross-border interaction and millions of users making it a boiling hot market. As always when the future of a market looks bright, there are certain risks to address.

Recently, we have seen different groups bringing down company websites and publishing confidential information. The majority of these attacks does not require much effort from the attacker but often give the victims bad publicity that is hard to get rid of. This is what the media love to write about. Even when attacks like these happen, they are in a minority compared to different system failures. Simple things such as malfunctioning equipment can quickly turn into a crisis when the effects escalate.

One recent example of where business continuity has failed was with a large outsourcing company whose customers were completely cut off from the service. This meant that people in Sweden could not get their prescriptions from pharmacies as a direct result of business continuity failure. One lesson learnt from this case was that it is good to have plans, but these plans need to be effective once disaster strikes which emphasises the acute importance of staff training – training that assumes realistic crisis situations. But how is this achieved?

The question, of course, is how to implement measures for business continuity that you can verify *before* the incident.

Business continuity focus

Business continuity is a definition that means different things depending on whether you are an IT-person or an executive. This is one of the reasons why it is complicated to implement business continuity from the business processes all the way though to the actual technical systems. On a higher level, business continuity is about ensuring that all of the processes in a company will continue to work as intended and thereby contribute to its development.

The first step: Defining the most critical assets

For any company, it is vital to be cost effective when it comes to implementing measures ensuring business continuity; therefore, it is important to prioritise business processes and assets. This is where the risk-based approach is used. Which assets are the most critical to business process, and what are the impacts on the business if the assets are not available?

The second step: Business continuity plan

Once your critical assets have been identified and documented as part of the standard risk management process within your company, it is important to produce and implement continuity plans for these assets. To ensure that the plans themselves are successful, an implemented continuity process in everyday business is key. This includes a business continuity policy setting the framework and goals together with an organisation process that defines clear roles and responsibilities.

The third step: Incident training and practice

Once the continuity plans and measures are in place, it is just a matter of waiting for a real incident to occur. Or is it? If you do not think that this approach is a proactive way to handle future incidents, you should schedule incident training as a natural part of staff training.

Once again, we return to the critical assets and construct realistic scenarios from the identified risks which potentially cause the worst impact. For example, if there is a critical business process with a high value risk of being disrupted by an external attacker, this risk should be enacted as part of a training drill, incorporating the continuity documentation, incident organisation, system owners as well as IT staff.

There are different ways to train before incidents occur, one being a table-top exercise and another being incident simulation. Table-top exercises are a good way to train staff who are responsible for relevant systems and processes through 'round table discussions' where a specific incident scenario can be addressed. For more real life training, there are also possibilities to simulate the incident environment with different people acting according to a predefined scenario.

Regardless of method, the best effect of training is achieved when all parts of the company are involved, from executives to IT technicians.

Conclusion

A successful business continuity programme is key to ensuring that a company will not be adversely affected by a disaster situation. It can even turn into an advantageous situation by increasing the trust of your trademark. Taking business continuity into account during your daily activities will help in reaching this goal.

The best way to be prepared is to be proactive by exercising worst case scenarios for critical business processes. Also, make sure you train for the Black Swan scenarios; you'll be surprised how often the impossible is in fact very possible. To implement incident training as natural part of the company is an investment in the future and helps everyone to be confident that no matter what incident occurs, the company will be able to handle it.

A well-structured business continuity training programme may actually be the one thing that prevents a minor incident from becoming a serious business failure. In fact, proactively securing business continuity might be the best way to address whatever the future may hold.

Jonas Stewén operates as Technical Sales Director and CTO within business area Information Security at Combitech, a consulting company with 1,300 employees. Jonas has been working with information security for more than 11 years and has performed multiple assignments from technical IT-security to managing information security for companies and larger projects for a wide variety of market segments.