



Expert from DataFort outlines five steps to take to prepare for a cyberbreach

At a time when cloud computing, mobile usage and IoT implementations are on the rise, it's important that organisations of all sizes know how to strengthen their security posture and be prepared for cyberattacks. Sachin Bhardwaj, an industry expert from DataFort, spoke to *Intelligent CISO* to offer his advice.



Sachin Bhardwaj, an industry expert from DataFort



loud computing, mobile usage and impending IoT implementations are all indicators of the higher risks involved in data breaches. Staying in a state of cybersecurity preparedness is crucial to any organisation that relies on data which is critical to their business.

This is true for organisations of all sizes, from governments to large enterprises as well as smaller companies. And this also cuts across the range of businesses from banking, healthcare, retail, transport, oil and gas, education, etc.

The Online Trust Alliance's (OTA) 2017 *Cyber Incident & Breach Trends Report* indicates that the number of cyberincidents doubled from around 82,000 incidents in 2016 to nearly 160,000 in 2017. What it also indicates is that 93% of these occurrences could have been prevented. This brings to light the gravity of the situation where organisations must remain focused on

their cybersecurity posture, processes and procedures.

The threats are growing in frequency as well as in the level of complexity. It is evident that, to curb the intensity of cyberattacks, companies must remain in a state of readiness to tackle targeted attacks. In such an event, it is important that they respond effectively to curtail data as well as economic losses.

Some of the basic aspects that need to be considered to ensure that organisations are prepared in the event of cyberattacks include:

Allocate proper budgets

Security comes at a cost. Be it hardware, software, constant upgrades, qualified staff etc, each of these elements must be given their due importance and should be considered to ensure a robust security system. While some organisations opt to invest internally, many organisations today are looking to outsource their security needs to third party providers.



Understand your risk profile

The risk profile outlines a company's known risks, policies and practices to guide how far you need to go and are willing to go to safeguard your assets and data. The most basic approach to understand your risk profile is to conduct an information gathering exercise and rely on internal resources.

A more professional alternative that produces more extensive insights is to hire a consultant or solution provider to conduct an external audit of your processes and infrastructure.

Prepare an incident response plan

In case of a cyberattack, organisations must have an incident response plan to tackle the issue at hand effectively. The basic goals would involve the creation of a team that has clearly defined roles and responsibilities. It would also be important to prepare basic rules and instructions in advance which must be followed to minimise damage.

And, in order for the information flow to reach out in a timely and organised manner, organisations must ensure that the right communication is shared at the most appropriate time across stakeholders including employees, supply chain, customers, etc to keep them abreast of the situation in hand as well as about the corrective measures underway.

Minimise downtime

Data is critical – it's the engine of any business activity – and its role and importance therefore must be placed at very high level within the organisation.

Its safety and security should play an integral role in the overall management strategy. The objective of any IT team in the time of a cyberattack is to ensure that there is business continuity

and the delivery of ongoing services. However, there must also be a strong consideration by the CEO and directors on a legal platform to ensure that their shareholders are not at risk.

Therefore, minimising downtime during an attack is central and can be dealt with by having the right business

continuity and disaster recovery plans in place.

Remain proactive

Timely skills upgrades are very relevant in today's changing cybersecurity environment. Training and communication must be provided on a



Develop a roadmap of your current security factors and prepare for future needs by bridging the gap with clearly defined objectives to be met within each growth phase.



Staying in a state of cybersecurity preparedness is crucial to any organisation that relies on data which is critical to their business.

regular basis, not just to the IT teams but across the spectrum of internal departments and customers. This will help in raising the resiliency of security for the entire organisation.

In conclusion, develop a roadmap of your current security factors and prepare for future needs by bridging the gap with clearly defined objectives to be met within each growth phase. Following cybersecurity best practices is a necessity to negate cyberattacks. ♦