IT security debt, it's a deep burn

By Stephen Osler

2 Apr 2020

If we can consider cyber threats as thousands of little digital fires that flicker in and out of a company's operational systems every day, think about the manpower required to manage these security alerts every time a possible threat is identified. It can leave an organisation in a state of operational duress rather than the company and its employees settling into a state of continuous improvement.

Stephen Osler, founder and business development manager, Nclose

It is a challenge to companies big and small, and this burden on employees and the company intensifies the more indebted a company is to its security operations. Security debt accumulates when cybersecurity issues aren't addressed early enough.

This puts companies behind the maturity curve, which leads to a myriad of secondary security issues. Protracted implementation phases of new technologies or projects is an obvious symptom of security debt issues.

We recently took full operational control of a large retailer's security technologies in a bid to eradicate their security debt. The company's IT security staff were skilled in implementing the technologies, but we assisted with implementation and took over the operational burden, which allowed the internal team to focus on improvement projects and initiatives. We also integrated with their response capability on the back of a Nview Managed Detection and Response (MDR) deployment, which elevated the response capability of our client, who knew exactly what to do when we identified a potential threat.

Following our recommendations and in deploying the Nview MDR, the retailer was able to focus on new projects and initiatives, leaving us to monitor and respond to the thousands of inputs that were triggered across their systems daily.

While underspending on security measures may not directly lead to deepening security debt or a security breach, it leaves a company with fewer capabilities that could have been directed towards improving maturity inside the business. Cyber fires and the manpower they require often burn away the potential for new projects and initiatives.

Cyberthreats don't discriminate

It's a persistent myth that cybercriminals only target larger companies. Smaller companies are often under greater security pressures than larger ones, as they can't afford to invest in the appropriate security systems.

When you find that operational teams are preoccupied and issues with vendor security products keep appearing, it may be time to relook your cybersecurity systems. It is one of the key reasons we offer free assessments: to ensure that the vendor products are being implemented properly to avoid these issues in future.

There are always ways and means for criminals to gain access to a system, but if you are constantly working on improving the state of your security operations, you are many steps ahead of those that don't. Let the firemen handle the fires so you can get on with business.

ABOUT THE AUTHOR

Stephen Osler, founder and business development manager, Nclose