

The Day that Never Comes... Minimising the Impact of Security Incidents



Few organisations are immune to security breaches. Despite their best efforts, IT security teams **cannot always prevent** an organisation from falling prey to an incident – anything from a targeted to a completely random, graffiti-style attack. Responsible IT management therefore calls for a thorough understanding of the vulnerabilities in your infrastructure and a strong focus on IT security incident management.

Vulnerability and IT security incident management are the cornerstones of a comprehensive risk management programme.

These interdependent concepts focus on reducing the organisation's risk by proactively searching for and managing vulnerabilities. At the same time, however, you need to accept that at some point in this process, failure is inevitable. Yet, the way you react to incidents will make all the difference to their level of impact on your business.

Detect vulnerabilities proactively

Vulnerability management is one area in a business where it is very difficult to measure success. As a result, security personnel run infrequent scans and oftentimes don't compare the results of scans to enable them to proactively manage the output.

Effective vulnerability management is neither reactive nor ad-hoc. It is a discipline that requires security personnel to scan for vulnerabilities on the network according to a strict schedule. Running regular scans enables you to establish a baseline and track changes to your risk profile. That said, the prospect of running a scan on 5,000 devices and finding 23,000 issues to deal with can be daunting. For these reasons it is critical to manage the output of your

scans by implementing procedures to prioritise, assign, remediate and track the identified vulnerabilities.

Bear in mind that the objective of vulnerability management is not to avoid attacks, but to proactively improve your organisation's vulnerability profile. As a first step, create a policy and procedure framework to support the vulnerability management process. The framework needs to include information on the tools and techniques you will be using to manage vulnerabilities, as well as the personnel who will take ownership of the process and the reporting tools which will be used. You should also develop a policy to set the objectives of the programme and to address issues such as end-user education.

A security incident becomes a reality

While you can take proactive steps to prevent incidents, ultimately, you need to regard them as inevitable. IT security incident management is an issue that needs to be addressed before the first major incident takes place or you run the risk of your IT team reacting instinctively, resulting in the impact of the incident being greater than it should be.

Anticipate and plan for security incidents by establishing a policy and procedure framework. The framework should ideally include:

- A definition of a security incident (what constitutes a security incident will vary from organisation to organisation)
- The method of reporting and recording an incident
- Allocation of responsibility for declaring, managing and escalating an incident
- The procedures prescribed by the CERT Coordination Centre which deals with major internet security problems, forensic procedures, as well as incident containment, eradication and root cause analysis procedures
- Detailed communication procedures, especially to authorities and the media

Reactive technologies

Most organisations have already invested in technologies to protect their infrastructures. However, vulnerability and IT security incident management cannot be addressed by through point solutions.

Policy and procedure frameworks for vulnerability and IT security incident management need to be supported by multiple layers of technologies for protection. For example, implement intrusion prevention technologies on the most sensitive network segments, servers and client devices to act as a reactive second layer of defence. Implement security event management to track and react to incidents.

The rationale is that if you have technology in place that stops the exploitation of the vulnerability, you can better plan the patch management lifecycle and reduce the exposure of your attack surface. In addition, the risk of the immediate exploitation of vulnerabilities can be reduced, as well as the danger of a rushed process to patch which could result in a similar impact to the organisation as a security incident if it goes wrong.

Fail to plan – plan to fail

By focusing on vulnerability and IT security incident management as part of your risk management programme, you can reduce the duration, severity and cost of incidents.

Bear in mind that the success of any security initiative is dependent on the support of the business. When an incident occurs, it is not only the concern of the IT department, but the entire organisation. Ensuring that your CEO and executive management understand the realities of vulnerabilities will go a long way toward ensuring the successful rollout of the necessary frameworks. The deployment of these frameworks can, in turn, mean the difference between a minor incident and a catastrophe.

MIDDLE EAST & AFRICA

ALGERIA • ANGOLA
BOTSWANA • GHANA • KENYA
MOROCCO • NAMIBIA • NIGERIA
SAUDI ARABIA • SOUTH AFRICA
TANZANIA • UGANDA
UNITED ARAB EMIRATES

ASIA

CHINA • HONG KONG
INDIA • INDONESIA • JAPAN
KOREA • MALAYSIA
NEW ZEALAND • PHILIPPINES
SINGAPORE • TAIWAN
THAILAND • VIETNAM

AUSTRALIA

AUSTRALIAN CAPITAL TERRITORY
NEW SOUTH WALES • QUEENSLAND
SOUTH AUSTRALIA • VICTORIA
WESTERN AUSTRALIA

EUROPE

BELGIUM • CZECH REPUBLIC
FRANCE • GERMANY
ITALY • LUXEMBOURG
NETHERLANDS • SPAIN
SWITZERLAND • UNITED KINGDOM

AMERICAS

BRAZIL • CANADA • CHILE
MEXICO • UNITED STATES