Managing security breaches...

**APPLICATIONS**

- Preparing evidence for litigation support.
- Fact-finding investigations.
- Investigate data loss and compromises.
- Safeguarding an organizations considerable interests.
- Planning and preparation for the impact of an incident
- Address threats, vulnerabilities, malware outbreaks, and cyber incidents
- Reducing the time between discovery and remediation
- Delivering timely and measured response with minimal business disruption
- Support executives with guidance on both internal and external response
- Execute remediation plans to prevent reoccurrence.

**INTENDED FOR**

- Law firms and solicitors.
- Financial institutions.
- Insurance companies.
- Corporate sector and industry.
- Investigative companies.
- Government agencies.

---

**Security breaches happen!**

There are a plethora of information security products and services available that all address pieces of the vulnerability landscape. However, no single technology or product will keep an organization 100% safe and secure. It is therefore not a question of if you will be attacked and suffer a security breach, but when and to what extent. Implications are that if a security breach occurs, it can easily escalate and becomes a traumatic experience, but it can also be an anticipated risk. This choice is totally up to your organization’s risk management strategy and planning.

**Vulnerability landscape**

Technology taking over many parts of the corporate world, has caused a shift with respect to the required capabilities and intentions of people and organizations with malicious intent. This shift has changed to such an extent that it is safe to conclude that all crime has directly or indirectly become computer crime. Hackers, cyber criminals, terrorists, disgruntled employees, and even nation states, just to name a few. Over the past years these groups have become efficient, persistent, and well funded organizations who’s mission it is to penetrate and compromise computer networks and automated information systems.

Their objectives are compromising trade secrets like intellectual property, financial records, customer data, and even the complete dismantling of your company’s critical business processes. Besides significant financial consequences, your organization can suffer a substantial loss in productivity, time, and reputation.

**Incident Response**

Incident response is an organized approach to addressing and managing the above mentioned (information) security breaches, and the aftermath thereof. It encompasses limiting negative effects, reducing recovery time, and identifying the person(s) and / or organization(s) responsible.

**Critical support when you need it most**

Xandstorm can provide Incident Response services both remotely and on-site to assist organizations mitigate their impact and recover critical business processes in a timely manner.