Identifying the Weakest Link in Data Security Defence

It is widely acknowledged that organisations who make efficient use of their data are better positioned to gain competitive advantage in the marketplace. Data like intellectual property, sensitive customer information and credit card data can be a huge liability to an organisation if it falls into the wrong hands, is leaked or left lying dormant on a network.

In helping to improve the efficient use of data while also enhancing data protection and compliance standards, one information security expert claims that organisations need to take heed from the U.S. Department of Defence (DoD). According to Andrew Serwin, CEO of The Lares Institute, a think tank focused on technology, privacy and information governance, ‘the cyber risk is an asymmetric threat –organised actors who try to use information against us, create an information imbalance to find the weakest link and then attack.’

That weak link may not necessarily be within the organisation. For instance, if a particular supplier doesn't follow the same security protocols as the company, an attacker could penetrate that supplier's defences and from there move up the chain into the network.

Information Superiority - Optimize Risk

According to Serwin, information and not technology is the underlying threat, and he advocates a doctrine that originated from the DoD referred to as information superiority. The DoD command and control their information domain, so if applying this theory to private industry, it means prioritising the superior use of information in order to minimise data risk, increase profit, reduce costs and protect against reputational damage.

The DoD consider information superiority as "a relative state achieved when a competitive advantage is derived from the ability to exploit information advantage" and as
‘the ability to develop and use information while denying an adversary the same capability.’

In order to achieve information superiority, the private sector needs to engage in technical and behavioural modification in how information is collected and processed in order to add value. The first step an organisation should take is to create a governance structure which includes key senior stakeholders from departments such as IT, privacy, human resources, audit, legal, treasure and security with the purpose of increasing the horizontal sharing of data in order to make information the main battery of business.

Information Assets Inventory

The first objective of any information governance group should include an information inventory to understand what data an organisation has and where it resides on a network. Once this stage is complete, an organisation should undertake a data classification exercise. According to Serwin, the intelligence community divides information into four categories: unclassified, confidential, secret and top secret and suggests the private sector adopt a similar scheme for protecting consumer data into non-sensitive, slightly sensitive, sensitive and highly sensitive. The point of classification is to focus data protection efforts in a structured and proactive manner.

Increased protection need to be applied to highly sensitive forms of data like social security numbers, passwords, credit card data, financial account information and other types of corporate critical data. ‘This allows companies to focus proportionally less resources on less sensitive forms of information and eliminate a lot of the problems with information if you focus on your most sensitive data’, Serwin added.

Share Information Horizontally

Once a comprehensive information inventory has been identified and classified, the information governance group should focus its attention on creating new ways to horizontally share information within a company while reporting back to senior leadership on its progress.

Concerns about information typically focus on subjects like privacy as organisations attempt to limit their legal exposure in the use of consumer data. Achieving information superiority has a
broader sweep than just privacy and needs to concern information that aid executives in also making decisions that drive revenue and reduce costs. Through sharing data horizontally, it will identify issues and opportunities that had previously been obscured, create greater efficiencies and deliver efficient data protection across an organisation.

In recognising what data assets exist within an environment, one of the first and most critical steps is to audit a network in order to ascertain what data it holds, assess its value and make informed decisions about how it should be managed, handled and stored. While no risk factor can ever be entirely eliminated, organisations that implement new interactive approaches to security awareness and procedures are finding that the payout is worth the investment. As employees learn how to identify and report vulnerabilities, they become invaluable to a company’s defensive, as well as offensive security posture.

PixAlert’s Data Enterprise Solutions help organisations to take inventory of critical data assets through a comprehensive Data Discovery process which is a vital first step in establishing a security protection framework. It enables businesses to easily audit-network resources and gain enterprise-wide visibility into ownership, location and usage of unsecured, critical corporate data while quickly identifying key risk factors. Only when an organisation has this level of visibility, can it begin to understand risk and vulnerabilities and execute the necessary corrective action to protect valuable corporate data assets.

Enabling Business To:

- Enterprise-wide visibility into the ownership, location and usage of unsecure data
- Quickly evaluate and identify key risk factors with highest exposures
- Empower users to take required action to protect data
- Ensure resources and efforts are directed to data with greatest value
- Optimise value and usability of unsecure data
- Improve compliance activity in a structured process
- Proactive and automated detection to real threats
- Measure Security Policy effectiveness and uptake
- Continuously enforce User Acceptance of existing controls and policies

For further information, see PixAlert’s Data Discovery capabilities or contact info@pixalert.com.

Article Source: Information Superiority / Computerworld
Author: Gerard Curtin, CEO, PixAlert

Date: 09 January 2013