Wikileaks: who is(n't) safe?

In light of the Wikileaks disclosures and the huge publicity they have engendered, what should companies do to protect their data?

The recent publicity resulting from the disclosures made by Wikileaks and the subsequent support for/ attacks on its founder Julian Assange have brought data security and cyber wars back onto the agenda of governments and company boards. No longer is data security the domain of technical specialists within the IT and Risk departments: espionage has gone mainstream.

Why the fuss?

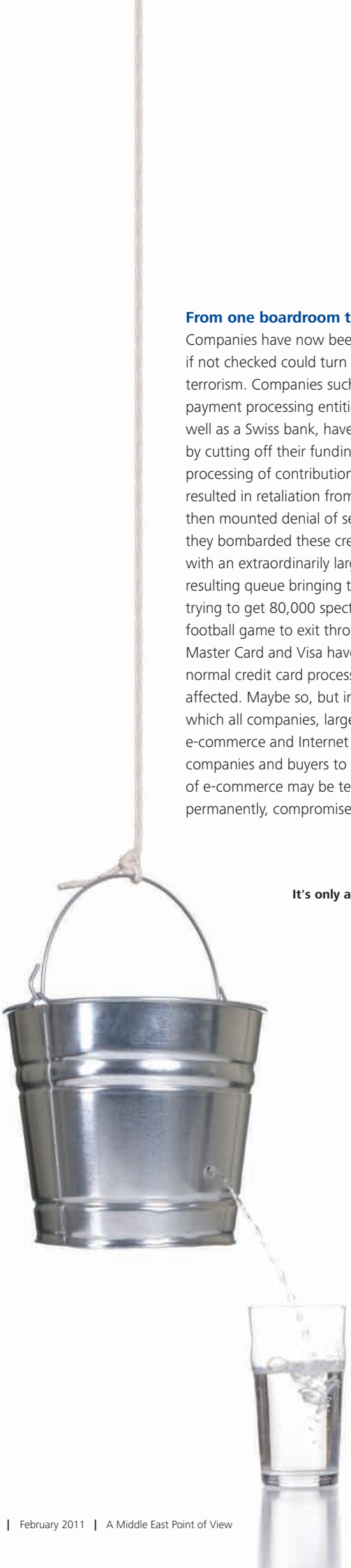
In view of the wealth of information that Mr. Assange and hence, Wikileaks have been provided with: electronic copies of minutes of meetings, e-mails and quotes made by diplomats, politicians and government officials - and now even former Swiss bankers - it seems that no discussion held behind closed doors or 'confidential' memo is guaranteed to remain so.

Supporters of Mr. Assange and Wikileaks believe that all the information released should be made public as diplomats and generally, government officials, should be held accountable for their words and actions both in front and behind, the microphone. Fighting corruption through extended transparency is to be applauded, they say. There are those, however, who believe that to allow governments to operate effectively and ensure national security, certain information should, and must, stay confidential.

Governments are understandably very irritated by these disclosures although none to date seems to have caused a great measure of embarrassment. The real fear is that as this information is released via 'slow drip treatment' the next or subsequent disclosure will prove politically damaging to a specific individual or country.

From one boardroom to the next

Companies have now been sucked into the fray, which, if not checked could turn into a war to fight cyber terrorism. Companies such as the major credit card payment processing entities of Visa and Master Card, as well as a Swiss bank, have tried to close down Wikileaks by cutting off their funding and stopping their processing of contributions to Wikileaks. This has resulted in retaliation from Wikileaks supporters who then mounted denial of service attacks on these entities: they bombarded these credit card company websites with an extraordinarily large volume of traffic, with the resulting queue bringing the website down. Imagine trying to get 80,000 spectators at the conclusion of a football game to exit through one single small gate. Master Card and Visa have been quick to say that normal credit card processing had not been adversely affected. Maybe so, but in the commercial world in which all companies, large and small, rely on e-commerce and Internet payment, it has caused companies and buyers to fear that their chosen model of e-commerce may be temporarily, or even permanently, compromised.



It's only a leak, but what if it pours?

And with good reason. Over the last Christmas spending spree, it was estimated that nearly 50% of all spending in the United Kingdom was over the Internet with credit card electronic settlement. Another study at a large IT security company, Avira showed that one out of every three of their users worldwide now accesses their financial accounts online.

With the increased use of the Internet for e-commerce and with more than half the Internet traffic now based on file-sharing it was only a matter of time before exchanged information led to embarrassing data leaks. With the continual development of mobile telephony services, there is also the fear that these security breaches may now spill over onto mobile devices and their supporting systems.

But the most significant risk to companies remains the release of confidential company information by employees. These exposures can lead to embarrassment and reputational damage, not to mention the loss of intellectual property that can result in a competitive disadvantage.

Some governments now feel compelled to act. The French Industry Minister called for a ban on French companies hosting Wikileaks sites leading supporters to cry 'foul' and to sabotage this attempt by relocating and copying the Wikileaks files many times to sites with different hosting names. In fact if the pressure on Mr. Julian Assange becomes too intense he can, through what is called a 'thermonuclear' option, release all his held information, so far still encrypted and kept secure, in 100,000 copies. Data experts have also warned the Canadian government that it, and Canadian companies (and I am sure this applies to all governments and companies) are vulnerable to data loss, on the same scale as the Wikileaks scandal that has rocked the United States government.

So what should companies do to protect themselves?

Solving potential security breaches requires a multi-faceted approach. Companies should start with a risk assessment exercise where ownership and classification of data is discussed and agreed upon. Sensitivity levels for each type of data should also be determined. Organizations can then decide 'how much' to spend to secure their data depending upon the level of sensitivity of each class of data.

Better education for all employees is also essential to ensure that they too, fully understand their role in ensuring the security of the company's key information and are held accountable for any breaches, whether accidental or intentional. A commitment is also required from senior executives and board members. Responding to cyber crime should follow the organisation's overall risk management approach. This way it becomes a regular item in the IT security and risk management budgets and on the agenda at management and board meetings. Specific action should start with intelligence gathering from external and internal intelligence feeds.

Most companies do not have proper data maps and so do not know exactly where all their key information is held or in fact if it has already been copied or replicated onto their staff's private date storage devices (USB drives or external hard drives) that are not subject to the company anti-virus and other security checks. By allowing staff to work on laptops and from home even, as most companies do and even encourage, they are allowing and even encouraging the spread of critical company information onto private devices.

In light of these significant potential risks of cybercrime facing every organisation, no single company irrespective of size can fight cybercrime on its own. Their response should be a process to prioritize threats, analyse threats, detect a threat before, during, or after it has occurred and specify the appropriate response. This layered approach should be applied to all information assets. These layers should include the introduction of strong and enforceable policies and procedures over and above the security awareness programs.

These enhanced governance steps must be backed-up by installing the latest security software. The IT security software industry needs to work with the national and international regulators to ensure that robust software that will prohibit data snooping and data sharing outside of internationally agreed strict standards is invented and introduced. Just as we have strict rules for driving on the roads with strong enforcement in most countries so we need governments, with the help of the global IT security industry, to ensure that the same high standards and rules are introduced and globally enforced on the information superhighway.

Just as we have strict rules for driving on the roads with strong enforcement in most countries so we need governments, with the help of the global IT security industry, to ensure that the same high standards and rules are introduced and globally enforced on the information superhighway.

Government regulators in every country should support this drive with well trained law enforcers backed up by meaningful criminal sentences for those who transgress these laws.

Conclusion

Public opinion is still divided on whether Wikileaks, or Mr. Assange in particular, is a virtuous global citizen or a cyber criminal. Be it as it may, no organization, private or governmental can ignore the risk of its information racing down the superhighway that is the Internet and should take adequate measures to protect itself.

by **Mark Dunn**, IT specialist group partner,
Deloitte in the Middle East

References

- Economist articles in the 11 December 2010 edition.
- US says it will take several years to secure its networks, as cybercriminals advance.
  The Canadian Press, 5 December 2010.
- Cybersecurity lax, experts warn; Government and industry are vulnerable to large scale los of data, they caution.
  Postmedia News, 1 December 2010
- With better sharing of data comes danger.
  The Washington Post, 29 November 2010.
- How Facebook could harm your business.
  The Star, 29 November 2010.
- Dangers of personal device use in workplace.
  SC Magazine, 11 December 2010.
- Avira Survey: 50% of People Wary About Banking Online.
  Wireless News, 15 November 2010.
- Cybersecurity; Everybody's imperative – Protecting our Economies, governments, and citizens Deloitte publication, May 2009.