intimus consulting is a division of the MARTIN YALE GROUP
Bergheimer Strasse 6-12
88677 Markdorf / Germany

www.intimusconsulting.com

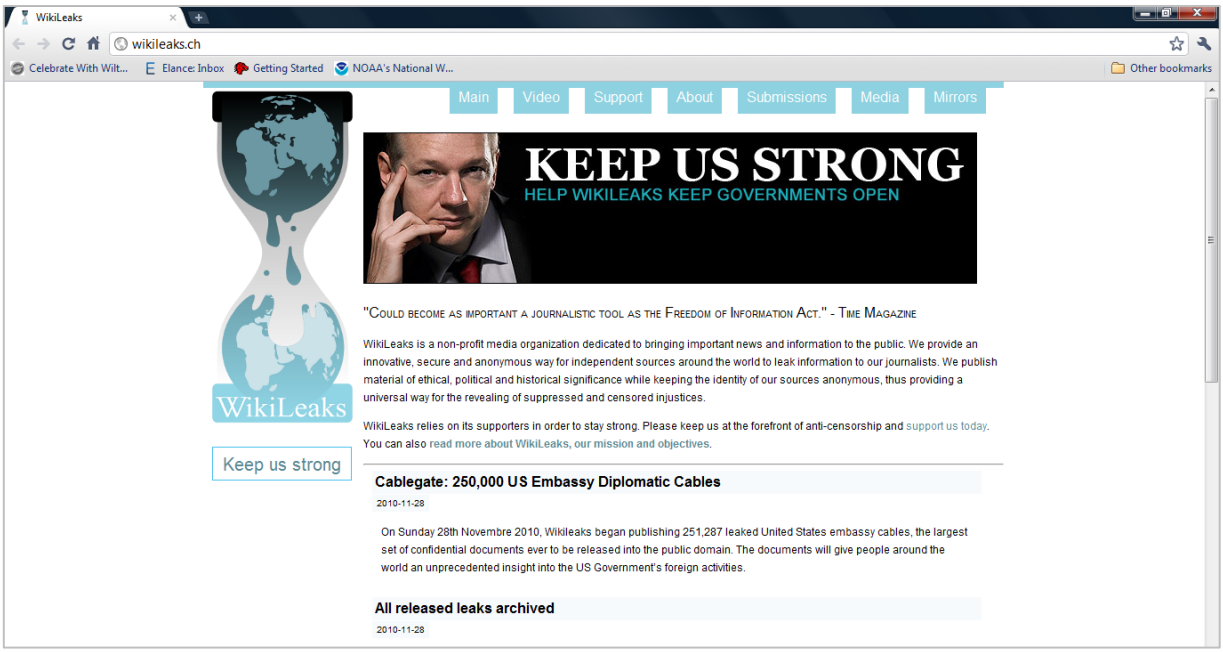
intimus®
SECURITY CONSULTING

Protecting against the weakest link: Information Security in the Age of WikiLeaks

Whitepaper

intimus®
SECURITY CONSULTING

Protecting against the weakest link: Information Security in the Age of WikiLeaks



Summary

WikiLeaks has come to international prominence (or notoriety, depending on your perspective) for its work in publishing private, secret and classified materials obtained via leaks from government sources.

WikiLeaks has published top-secret information from the U.S. military's wars in Iraq and Afghanistan, and has also shared thousands of pages of U.S. State Department cables with the world.

The U.S. government and other governments around the world are learning that in the age of WikiLeaks, no secret is safe.

What does this mean to your company or organisation? This white paper shows a few lessons of WikiLeaks for information security leaders in today's business and government organisations.

intimus®
SECURITY CONSULTING

Content

Information travels fast

Daniel Ellsberg
(source: Wikimedia Commons)

In 1971, U.S. military analyst Daniel Ellsberg, having grown disillusioned with his country's war in Vietnam, decided to leak a set of confidential military documents called "The Pentagon Papers" to the New York Times and other newspapers.

The Pentagon Papers was a secret official history of the U.S. government's decision-making and escalating involvement in the Vietnam war; its publication helped to decisively turn public opinion against the war and led Daniel Ellsberg to be prosecuted for espionage (he was later released following a mistrial).

In 1971, leaking such a vast quantity of sensitive information was a complex and time-consuming process. Daniel Ellsberg spent hours secretly making photocopies of over 7,000 pages of documents, which he covertly delivered (in person) to contacts at various newspapers and in the U.S. Senate. In 1971, it took time and effort and physical space to manage so many thousands of pages of information.

Today, in the Age of WikiLeaks, information is practically invisible, travelling over broadband and cloud applications. Instead of Ellsberg's copy machine and stacks of paper documents, WikiLeaks traffics in secure servers and encrypted e-mails. Instead of being shared with a few newspaper reporters, confidential information today can be posted online and be viewed instantly by millions of people worldwide.
The information that your company or organisation would most like to keep secret can be disseminated, copied and shared more widely and easily than ever before. Have your information security protocols kept up to speed with these latest developments?

Protecting against the “least trusted person”

Just as a chain is only as strong as its weakest link, as security technology expert Bruce Schneier says, “secrets are only as secure as the least trusted person who knows them.”[1] WikiLeaks was able to disseminate confidential information to a worldwide audience, faster and more efficiently than ever before – but WikiLeaks did not get their information in a “high tech” way – they got it by an old-fashioned leak from some person inside the organisation who decided to violate his/her security clearance and share secrets with the outside world.

Who is the “least trusted person” at your organisation? What is the “weakest link” in your organisation’s information assurance protocols and programs? Do you have controls in place to make sure that sensitive information is only available to a select group of people who have a “need to know? Do you have information classified appropriately according to its level of confidentiality, and is that information managed appropriately based on the risk it poses to the organisation?

Every aspect of your organisation’s operations, from hiring to training, from online network passwords to whether employees are allowed to bring personal media storage devices to work, to how waste paper is disposed of at the end of each working day, can be managed in a way that reduces the likelihood of a damaging data breach.

[1] Schneier, Bruce. http://www.schneier.com/blog/archives/2010/12/wikileaks_1.html

Watch for warning signs of a data breach

The Verizon Security blog commented on the WikiLeaks story by saying that WikiLeaks' methods were not new or surprising – Bradley Manning, the U.S. soldier believed to be the source of much of WikiLeaks' U.S. military information, had shown many of the classic signs of being an information security risk.

As Verizon's blogger wrote, "The actions of Manning bear many of the hallmarks we so often see when analyzing breach cases. Too much privilege, low accountability, odd or anomalous activities, prior history of questionable behaviour, resentment, and/or frustration, use of personal media/devices, discovered/reported by an external party, and the list goes on."[2]

- **Too much privilege:** Although he was a low-ranking intelligence analyst (Private First Class) and was only 22 years old, Bradley Manning had workstation access to the SIPRNet – the Secret Internet Protocol Router Network used by the U.S. Department of Defense and Department of State to transmit classified information.
- **Prior history of questionable behaviour:** Bradley Manning had been reprimanded in 2009 for assaulting a fellow soldier, resulting in a demotion from Specialist to Private First Class. In a series of chat posts that were later published in the Washington Post, Manning said that he was facing discharge from the Army for an "adjustment disorder."[3]

  If your organisation has people in positions of access to sensitive information who have shown signs of behaviour problems, lack of respect for the organisation, or who just do not fit with the goals and standards of the organisation, perhaps it would be better (for both parties) to transition them out of the organisation rather than let them stay on and potentially pose an information assurance risk.

[2] Baker, Wade. "William H. Murray editorial on WikiLeaks." Jan. 4, 2011. http://securityblog.verizonbusiness.com/2011/01/04/william-h-murray-editorial-on-wikileaks/

[3] Nakashima, Ellen. "Messages from alleged leaker Bradley Manning portray him as despondent soldier." http://www.washingtonpost.com/wp-dyn/content/article/2010/06/09/AR2010060906170.html

To be sure, not every disgruntled employee goes on to create a data breach, but employees who are not happy with their jobs are a greater risk to make mistakes, fail to follow procedures, or commit other errors that could lead to an inadvertent data breach. With information security, "sins of omission" can be just as damaging as "sins of commission."

- **Resentment and/or frustration:** In the time leading up to his alleged leak of documents, Manning's Facebook posts indicated that he was frustrated with life, isolated at work, angry with the military, and depressed by his career prospects.[4] Disgruntled or malcontent employees who are dissatisfied with their lives and careers are often the biggest risks for data breaches – and these warning signs are often noticed by co-workers and supervisors. Does your organisation have procedures in place to watch for behavioural signs that could be "red flags" for information security risks?

- **Use of personal media/devices:** Manning took personal CD-RWs containing music to his duty station, erased the CDs, and rewrote them with the downloaded classified documents. Manning described the U.S. military's information security as "vulnerable…kind of sad…weak servers, weak logging, weak physical security, weak counter-intelligence, weak signal analysis…a perfect storm."[5] Organisations need to enforce strict policies regarding employees' use of personal media storage devices – whether you want to ban all personal storage devices, or have a policy with some exceptions, there needs to be a policy in place that clearly outlines the expectations for employees and that provides an appropriate level of security for the organisation.

[4] Heidi Blake, John Bingham and Gordon Rayner, The Telegraph, July 30, 2010, published online at http://www.telegraph.co.uk/news/newstopics/politics/defence/7918632/Bradley-Manning-suspected-source-of-Wikileaks-documents-raged-on-his-Facebook-page.html [cited January 27, 2011]
[5] Wikipedia, published online at http://en.wikipedia.org/wiki/Bradley_Manning [cited January 27, 2011]

- **Discovered/reported by an external party:** Bradley Manning was discovered not by Army intelligence officials or the CIA, but was reported to the authorities by Adrian Lamo, a former hacker who Manning had contacted and corresponded with after Lamo was profiled in *Wired* magazine. Many organisations do not realise that their data security has been compromised until they read about it in the news media. Does your organisation have procedures in place to serve as an "early warning system" for data breaches? If confidential information were to be leaked from within your organisation, how would you know?

In retrospect, it seems incredible that such a young soldier with a less-than-perfect disciplinary record had easy and unsupervised access to so many hundreds of thousands of confidential documents. Daniel Ellsberg was a senior military analyst with privileged access to secret government files, and he had to spend hours photocopying 7,000 pages in order to create the Pentagon Papers; Bradley Manning walked out of his workspace with a few CDs containing the largest data breach in U.S. military history.

Hindsight is 20/20, but one lesson of WikiLeaks is that organisations need to re-examine their policies to ensure that not all the most privileged information is available to all parts of the organisation. The more people have access to information, the more likely it is that the information will be disclosed – just as a chain is only as strong as its weakest link, secrets are only as safe as "the least trusted person who knows them."

The cost of data breach – or even a rumour of data breach – can be huge

In November 2010, WikiLeaks claimed that they had 5GB of data from a Bank of America executive's hard drive – and were planning to release the information. Even though no data had yet been released, Bank of America's stock fell 3% on the news.[6] The same "old fashioned" data breach techniques that led to WikiLeaks' revelations of U.S. government secrets could also be used to compromise the confidential data of private sector companies – all it takes is a single hard drive to fall into the wrong hands, or to be handed over by single a disaffected employee.

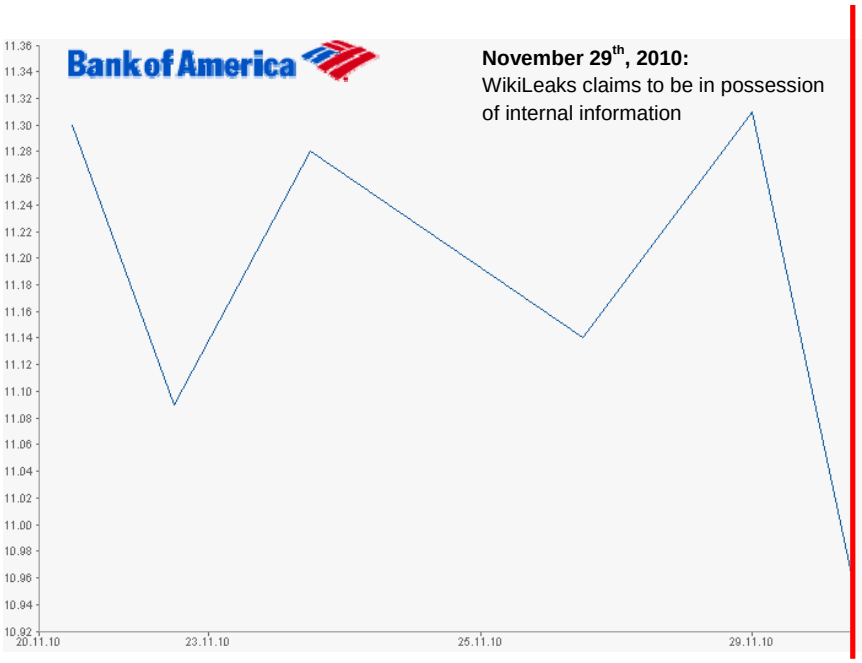


Chart 1: generated through www.finanzen.net

[6] John Carney, CNBC.com, "Bank of America's Risky WikiLeaks Strategy," Dec. 2, 2010, published online at http://www.cnbc.com/id/40471184/Bank_of_America_s_Risky_WikiLeaks_Strategy [cited Jan. 27, 2011]

Information security is not just about technology

Although better technology or more sophisticated security systems could have possibly prevented Bradley Manning's unauthorised disclosure of data to WikiLeaks, technology is not the only part of the solution. As Christopher Porter wrote on the Verizon Security blog, "Security technology is not a panacea. It's a process, of which, technology is only a piece of the puzzle…in the majority of incidents, the technologies and evidence of breaches are already in place, but nobody is looking for it."[7]

Many of the tools that organisations need to use for better information security have little to do with "technology" and more to do with rules, controls and limits on access to information. The Verizon security blog says that in 2011, they hope to see "a shift toward actual adoption of well-known but not-so-well-adhered-to concepts like least privilege, need-to-know, and accountability."[8]

- **Least privilege:** Individual users should only have the level of access necessary to do their jobs. A 22-year-old Private First Class had access to hundreds of thousands of decrypted U.S. State Department cables. In retrospect, this was an embarrassing oversight – why did so many people need to have access to those files, which were not related to or necessary for their jobs? Does your organisation have any "oversight errors" like this, where sensitive information is accessible by people who don't need to know it?

[7] Christopher Porter, "Security Can Not Be Addressed by Technology Alone," Dec. 6, 2010, published online at http://securityblog.verizonbusiness.com/2010/12/06/security-can-not-be-addressed-by-technology-alone/ [cited Jan. 15, 2011]

[8] Wade Baker, "William H. Murray editorial on WikiLeaks," Jan. 4, 2011, published online at http://securityblog.verizonbusiness.com/2011/01/04/william-h-murray-editorial-on-wikileaks/ [cited Jan. 15, 2011]

- **Need-to-know:** Sensitive information should be classified only to those people within the organisation who have a specific need to know it. The concept of “need-to-know” restricts the ability of people to “browse” through sensitive information (as Bradley Manning allegedly did with the thousands of State department cables). How good of a job does your organisation do in limiting sensitive information only to those individuals who need to know about it?

- **Accountability:** Every level of the organisation needs to have plans in place to train your people about information security and reinforce the key concepts of least privilege, need-to-know and classifications of varying levels of confidential information. People at all levels of your organisation need to know their roles and responsibilities in handling sensitive information, and need to know what to do if they encounter information that is beyond their “need to know.” The best defence against data breaches is thorough, constant training to ensure that your team knows how to manage sensitive information appropriately and knows how to protect against data breaches. Even a policy as simple as “do not bring personal data storage devices to work” can help prevent accidental (or deliberate) data theft or data breaches.

Keep good products and systems in place

Fortunately, your organisation is not alone in confronting the risks posed by data breaches. Partners like intimus Consulting are available to help your organisation develop the right information assurance systems and identify the right products to help maintain your data security. intimus Consulting regularly helps our clients to take a holistic approach to information assurance, with processes including:

- **Define information "Security Zones"** ranging from "Public" (mailroom, print shop, archives) to "Restricted" (internal and external correspondence) to "Confidential" (sales, marketing, purchasing) to "Top Secret" (executive suite).
- **Destroy information safely and securely** to prevent unauthorized data from leaving the organisation – using products such as paper shredders, disintegrators, degaussers, and other data sanitization machines.
- **Perform risk assessments,** vulnerability analyses, implement information protection programmes and perform ongoing monitoring.
- **Create a customised Risk Matrix** for your organisation, including the various information security risks and the potential costs in case of a data breach.

Conclusion

With the many headlines about “hackers” and “identity theft,” it’s easy to think that information security is a high-tech game full of shadowy actors and highly complex technology. But the truth is that most data breaches and information leaks are caused from within the organisation by real people, who choose for various reasons to undermine their organisations and violate their trust.

If your organisation wants to avoid becoming the next target of groups like WikiLeaks, it’s helpful to remember a few key principles. Remember that your secrets are only as safe as the least trusted person who knows them. Pay attention to rules, processes and controls on access to information, not just “information security technology.” And remember that to ensure information security, it helps to have a holistic approach that measures the full picture of risks and vulnerabilities facing your organisation.

Information security is, in large part, a matter of maintaining trust. And every organisation has to contend with people who are willing to betray that trust – this is an eternal part of human nature and the human condition. But every organisation needs to take the proper precautions to make sure that a violation of trust does not lead to massive repercussions and worldwide scrutiny of sensitive information.

Company Profile

Data protection was something unheard of when the first shredders were introduced in the 1960's. Starting with the "electronic wastepaper basket" INTIMUS Simplex in 1965 the product range nowadays meets all the requirements imposed with regard to information assurance. It does not only contain devices for the shredding of classical data media, such as print outs, computer lists or even complete folders, but also features machines to destroy information on modern endpoint devices like CDs, floppy disks, Hard Disk Drives and Solid State Media.

intimus Security Consulting is a concept to assist organisations worldwide to define, implement and monitor procedures for information security beyond the endpoint.
More information is available under www.intimusconsulting.com.

The MARTIN YALE GROUP was formed in 2003 by the former individual organisations MARTIN YALE Industries (North America) and Schleicher International (Germany). Today the Group has got an extensive worldwide distribution network with 7 branch offices and over 150 distributors.

Contact Details

MARTIN YALE GROUP
Bergheimer Strasse 6-12
88677 Markdorf / Germany
Tel. 0049 / (0) 75 44 / 60-232
Fax 0049 / (0) 75 44 / 60-248
mailto: sattel@martinyale.de
www.martinyale.de