

## Policies, systems, software essential to prevent leaked data

In 2010, data breaches cost affected companies \$7.2 million on average

By SHEILA LIVADAS

**H**everon & Heveron CPAs has never been wikileaked, but it uses encryption, data monitoring, confidentiality agreements and other measures to prevent that from happening. The Rochester accounting firm's information would be worth more if it were released privately instead of publicly, but vigilance is still necessary, Vice President Michael Desmond says.

Preventing leaks of private, secret or classified documents to the Internet requires technology and sound organizational policies, information security experts say. Firewalls and spam filters are not first lines of defense because the threat typically germinates inside organizations.

Information security experts say businesses of all sizes should take seriously the risk of wikileaking—after WikiLeaks, the original whistle-blowing and news-leaking website founded by Internet activist Julian Assange. Though rogue employees who walk off with client lists, intellectual property or research and development plans usually attempt to make a profit, bruised egos or spite could prompt them to splash the information across the Internet.

Research from security software developer Symantec Corp. and the Ponemon Institute shows that data breaches are hurting firms' bottom lines. In 2010, affected companies paid on average \$7.2 million—or \$214 per compromised record—to clean up the incidents, and that was an increase of \$10 per record from 2009.

Preventing wikileaking begins with establishing access control, a system that permits an authority to monitor and limit access to areas and resources on computers.

"In the absence of that, you really don't have security," says Jonathan Maurer, executive director of the Information Security Office and Global Risk Management Services at Rochester Institute of Technology.



Photo by Kimberly McKinzie

**Preventing wikileaking requires employers to stand firm on security policies, says Sitima Fowler, CEO of Capstone Information Technologies Inc. She and her husband, Michael, who is president of the firm, advise clients to trust employees, "but you should always verify."**

Once basic access control surrounds sensitive information, more sophisticated technology can ratchet up security even further, Maurer says. Options include electronic auditing tools that can track who is looking at documents or digital perimeters that trigger alerts if data moves beyond certain boundaries.

Sound organizational policies also help thwart wikileaking, says Maurer. He is also an adjunct professor of enterprise security at RIT's B. Thomas Golisano College of Computing and Information Sciences.

Businesses can mitigate exposure by granting access to sensitive information on a need-to-know basis.

Dividing employees' roles and responsibilities is another safeguard to consider, Maurer says. Doing so may have upfront costs, but the return boils down to improved asset and risk management.

Records retention policies also play a role in preventing wikileaking. Technology exists that can place expiration dates on documents, but using it has to be weighed against the need for information to be available, he says.

Archiving email to prevent wikileaking could be a double-edged sword, Maurer notes. Whether individuals archive email on their own laptops or a company's information technology staffers use a central repository to do so, both practices raise security questions that need to be addressed.

"That's why I think a carefully crafted records management policy is another key foundational element to security," he says.

Sitima Fowler, CEO of Capstone Information Technologies Inc., says she sometimes encounters small-business owners who believe their employees would never intentionally jeopardize private data.

“But it’s still our job to point out that it’s good to trust, but you should always verify,” she says.

Small-business owners who are hesitant to invest in information security should consider what it would mean if they lost just 10 percent of their clients because of a data breach, says Fowler, whose clients include Heveron & Heveron.

Preventing wikileaking often requires employers to stand firm on certain policies, Fowler says. Because many smartphones now have the storage capacity to hold entire databases, employers should not allow employees to connect their devices to company networks.

Thumb drives, smart drives and writeable media also could easily be used to set a wikileaking plan in motion, “yet these can easily be controlled and audited—and should be,” she says. Disgruntled employees may even resort to low-tech methods to nab information, including rifling through trash bins or paper file folders, she adds.

Since email usually contains the information wikileakers find most valuable, investing in keyword-scanning software makes sense for some businesses, Fowler says. The software allows authorized users to limit who within a company receives email with sensitive content and also prevents unauthorized users from sending the messages outside an organization.

Tim Trueblood, chief technology officer for Rochester cloud-computing provider ExtraDev Inc., says employee training also helps prevent wikileaking. Entry-level human resource employees may not realize initially that they should not discuss or treat private data casually.

Though more companies are putting data into cyberspace with cloud computing, the technology itself is not vulnerable to wikileaking when operated with adequate controls, Trueblood says. Small private clouds, he adds, probably do not hold much allure to wikileakers, especially when compared to Facebook and other large-scale information repositories.

Still, “you have to know who your cloud



Photo by Kimberly McKinzie

**Preventing wikileaking begins with establishing access control, says Jonathan Maurer, executive director of the Information Security Office and Global Risk Management Services at Rochester Institute of Technology.**

vendor is and what their capabilities are and what they’re retaining for you, too,” Trueblood says.

When mounting a defense against wikileaking, “you just can’t go throwing money at the problem,” says Christopher Karr, president of UberGuard Information Security Consulting LLC. Assessing threats to sensitive data should be an ongoing process “because what’s secure today is not secure tomorrow.”

To ensure that employees do not have too many safeguards impeding their efficiency, information security experts and IT administrators need to work together, Karr says. Some security strategies, such as archiving email and attaching expiration dates to documents, have pros and cons, he adds.

Though Assange’s WikiLeaks has been inoperable for months because of the dis-

abling of its submission platform, spin-offs have emerged. OpenLeaks.org, launched by the Assange associate who crippled WikiLeaks, expects to be fully operational this year and—unlike its predecessor—will not publish information but will enable third parties to do so.

Despite emerging platforms for exposing private information online, some information-security experts do not expect wikileaking in business settings to grow by leaps and bounds. The chance to profit from selling sensitive data will likely keep the number of cases in check.

“Once it’s put out there publicly, in some sense it loses a lot of its value,” RIT’s Maurer says. “The genie is out of the bottle, and you can’t put it back in.”

*Sheila Livadas is a Rochester-area freelance writer.*