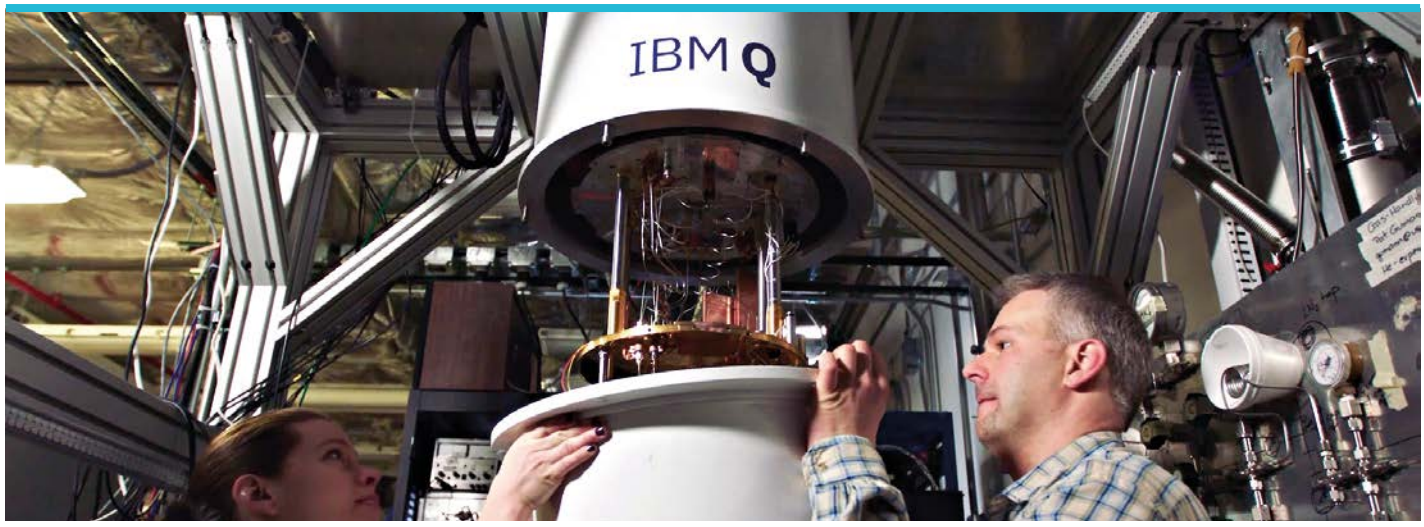


Image credit: IBM Research

They're here

Hackers can and do penetrate most IT systems. But organisations are getting smarter too, according to speakers at ISACA's recent conference in Munich

BY ARTHUR PIPER

Towards the end of this year, we could reach the point at which quantum supremacy has been demonstrated. If you have never heard of it, you should pay attention now. It marks the date when scientists will have built a quantum computer that has the potential to be more powerful than any other supercomputer on the planet. It could also mark the date when the encryption that most businesses use to protect their important data becomes useless.

> **Given the user address for a Bitcoin, for example, a quantum computer could work out the security code that protects the money from being stolen in a couple of minutes**

CHALLENGES TO QUANTUM-SAFE SECURITY

- It takes several years of cryptanalysis for cryptographers to gain confidence in the security of new algorithms
- Some network security protocols may be too rigid to accommodate the increased key lengths or changes in ciphers required to make them quantum-safe
- New standards for protocols are needed
- Many people perceive quantum-safe cryptography as "not urgent," despite the lead times required to analyse new cryptosystems and implement them in security protocols and products

Source: *Mike Brown, ISARA Corporation*

> **When you ask managers how many clients would they would lose from a data breach, how much market share and money, it soon gets very tangible**

Google's 50 qubit quantum computer will be ready this year, the company says. IBM expects to sell commercial 50 qubit computers in the next couple of years. Both machines will be game changers.

"We are in a similar situation to the Y2K fiasco," Mike Brown, ISARA Corporation's chief technology officer and co-founder, told the ISACA conference. In the rush to the end of the last millennium, companies spent hundreds of millions of pounds to ensure that their computers did not stop working when the clocks turned to zero on 1 January 2000.

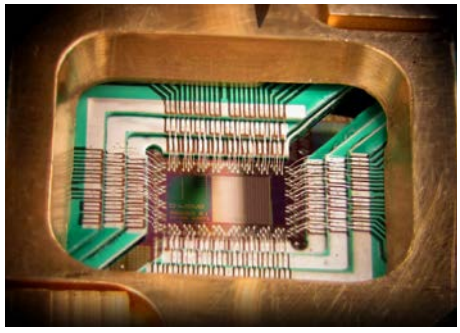
Y2Q – as Brown called it – could have a similar impact because quantum computers work differently to standard computers. They solve different types of problems – and are especially good at breaking codes. Given the user address for a Bitcoin, for example, a quantum computer could work out the security code that protects the money from being stolen in a couple of minutes.

The problem is not necessarily that all encrypted data will be automatically open for anyone to use – the issue today is that many organisations do not know what data relies on encryption and what does not. If they are storing data today that needs to be safe for beyond Y2Q, that needs to be assessed soon for its ability to be safe when quantum computing becomes commercially available.

"Organisations need to do a risk management assessment of all protocols and clients, and servers need an in-depth review," he said. "This requires coordination between vendors, OEMs and customers to catch all of the interactions."

The data most at risk includes any encrypted data where the key to unlocking it is communicated or stored along with the data, digital documents with a long shelf life, and signed software. The most difficult part will be to secure those transactions where different systems need to talk to each other because they often rely on public encryption protocols. "Interoperability will be the killer," he said. And while quantum encryption will probably come along, it is unlikely to be rolled out quickly enough for many organisations.

Image credit: D-Wave Systems, Inc.



Above: A chip constructed by D-Wave Systems Inc. designed to operate as a 128-qubit superconducting adiabatic quantum optimization processor.

Previous page: IBMers Sarah Sheldon and Pat Gumann working on a quantum dilution refrigerator.

Art of war

"IT security is a grave concern for a company and must be thoroughly studied," Tom Madsen told the conference – an IT specialist who worked for the United Nations Development Programme for 12 years. He was paraphrasing the ancient Chinese strategist Sun Tzu and his classic warfare text *The Art of War*. "IT is the foundation for what we do," he added.

He said that external threats were often not treated seriously enough from a risk perspective. Quite often, businesses patched and mended their security systems after minor incidents rather than undertaking a full forensic investigation to make sure that the attack had not uncovered a more important flaw in the organisation's defences.

"Every time we take a decision on the system, we are changing our risk profile," he said. "For example, are you changing the antivirus program because you have a better offer, or because you are looking for better security?"

Since all warfare is based on deception, he said, employee training on a regular basis was the key to limiting risk from cyberattack. "Whatever you do in training must

be done again and again and again," he said, "because if you do not have staff who are properly trained, or policy and procedures in place to help staff know how to act, you are leaving yourself wide open."

Business focus

"Full business engagement is essential to provide an appropriate and sufficient protection to business' most critical IT resources," Paul Phillips ISACA's Technical Research Manager said. But that was not an easy task. "This is not just about cyber security but engaging busy leaders who want to do the right thing but have other priorities outside of cyber security."

He said that it was essential for risk managers and cyber security experts to approach the issue from a business perspective. When a breach happened, for example, executives seldom wanted to know the technical details. Instead, they focused on issues such as how much it would cost, how quickly it could be put right, and whether there were legal and reputational issues to address.

Phillips said that cyber risk should be considered as an enterprise-wide business risk – without IT systems it could not be business as usual. As well as risk professionals helping to develop a common, business-oriented language, they needed to be able to demonstrate the return on investment expressed in hard cash terms.

"We need to articulate risk by focusing on the impact – not just threat or risk – and express that in dollars," he said. That would require risk and IT leaders to speak to people in the business and ask difficult questions. For example, how could a security breach damage reputation and stock value? "Ask them how many clients would they would lose, how much market share and money. It soon gets very tangible," he said.

Machine learning

While people are key to an effective cyber defence strategy that ties security and business objectives together, machine learning technologies are beginning to help organisations combat hard-to-detect attacks.

Last year, for example, an international sports company installed sophisticated video conferencing equipment to support its ever-growing number of overseas teams. But a hacker managed to gain control of a conferencing camera and use it to take out large volumes of data from the business' network. Such attacks can take months to detect and the breach left the company open to corporate espionage, ransom and several other threats.

Using machine learning technologies developed by a Cambridge-based company called Darktrace, the company could detect unusual data flows from the camera. The software models a system's behaviour from scratch with no pre-defined parameters. It builds up a picture of the network showing how data flows through the business and then analysts can dig deeper into the detail if they detect anomalies.

"The software is building up a pattern of life for the network," says Darktrace's Sam Alderman-Miller, "which acts as a norm against which we can detect unusual behaviour without interfering with the normal running of the business. As the company changes, so the patterns of what constitute normal will change."

The aim of such machine learning techniques is to develop a pattern of behaviour across the network that can be monitored in real time. The system can also wind back the time clock to see which other machines and devices the compromised network has been communicating with making it easier to trace where any lost data has gone.

The good old days of focusing all of your corporate effort in preventing a breach seem like a thing of the past. "The battlefield is now inside corporate networks and it is no longer sufficient to rely on a perimeter to secure the soft interior," Alderman-Miller said. Companies are going to need all the tricks in the book to keep in front of developments that are right on their doorsteps. ER

ISACA is an independent, nonprofit, global association for IT professionals: www.isaca.org. Enterprise Risk would like to thank ISACA for its hospitality in Munich.

BUSINESS DRIVEN SECURITY STRATEGY

- Prioritise assets and understand their vulnerabilities
- Quantify business risk and impact if those assets were compromised; determine if your budget is allocated properly
- Build a strategy to defend those assets with clear cost/benefit relationships outlined; make sure your strategy is holistic (people, process, technology)
- Determine gaps between what you have in place today and your ideal state
- Take a phased approach to addressing the gaps, but start today; prioritise according to impact on risk posture
- Constantly re-evaluate threats and vulnerabilities to tune your strategy; have a response plan in place

Source: *Paul Phillips, ISACA*

> **The battlefield is now inside corporate networks and it is no longer sufficient to rely on a perimeter to secure the soft interior**