WSJ. CUSTOM STUDIOS

CXOS' QUICK GUIDE TO 2020
NEXT-GEN CYBERSECURITY

SECURITY

Sponsored by NTT Communications

Cloud could be the Game Changer in Cybersecurity

By Peter Purton

BEING ABLE TO IDENTIFY ATTACKS AND COMPROMISED MACHINES WILL ALLOW ORGANIZATIONS TO TAKE ADVANTAGE OF PREVIOUS INVESTMENTS IN INCIDENT RESPONSE.

The year 2013 was not a particularly good one for those entrusted with the security of data systems. American retail chain Target lost 110 million of its customers' financial details. Some 150 million customer email addresses, encrypted passwords and password hints were stolen from software maker Adobe. And then it emerged that Edward Snowden stole sensitive data from his government employers. Since 2013, he and the impact of his actions have rarely been out of the headlines.

Rik Turner
Senior Analyst, Ovum

Since 2013, the data security challenge has become even greater. The number of data attacks has almost doubled, costing many more companies billions of dollars as well as reputation damage and loyalty loss. And they are getting more sophisticated.

"The ability of hackers and other malevolent forces to create new threats is growing exponentially"says Rik Turner, senior analyst in the infrastructure solutions team specializing in IT security at London based research and consulting business Ovum.

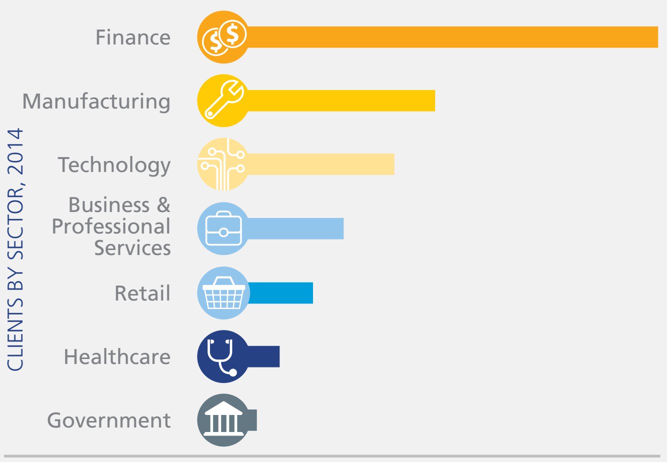
FINANCIAL SECTOR UNDER ATTACK

According to data gathered by NTT Communications for its '2015 NTT Group Global Threat Intelligence Report', finance continues to be the most targeted sector with 18 per cent of all detected attacks. But business and professional services are rapidly rising up the ranking of industry sectors where security is under threat, moving to 15 per cent from nine per cent. "Business and professional services increases are the result of the risks inherited through business-to-business relationships", said the report's authors in their summary.

> “Security on user premises versus that of systems in the cloud is like comparing physical security in an office block with that of a shopping mall”

The very interlinking and opening up that are necessary for business growth are also making it vulnerable, says Mr. Turner. "Target's data was stolen after the thieves compromised the credentials given to an air conditioning company serving its stores. But once you're in, you're in." And although Edward Snowden was just a contractor, he seemed to have had access to a tremendous amount of the National Security Agency's data, he adds.

SEVEN MOST VULNERABLE SECTORS



2015 NTT Group Global Threat Intelligence Report Copyright 2015 NTT Innovation Institute 1 LLC

The security situation is exacerbated by more people working from home, says Turner. Sometimes organizations don't even know what their employees are using with such excellent and tempting third party services like Dropbox, Box, Onedrive and Evernote easily available.

NEW MODELS FOR THE NEW CLOUD

The move from information systems hosted by organizations on their own premises to the use of cloud based systems is also changing things. In fact, the cloud requires a completely new security paradigm says Salman Ali, principal at management consultancy Arthur D. Little in Madrid.

"Security on user premises versus that of systems in the cloud is like comparing physical security in an office block with that of a shopping mall" he explains. "In an office block there's a security man at a desk near the front door, controlling who and what comes into the building. In a shopping mall there's no security at the front door, but lots of vigilant and visible guards observing and intervening when necessary."

Ali argues that information and communications system security is following a similar path, and will so more and more enabled through technologies like software defined networking and network function virtualization.

An obvious example can be found in how anti-virus protection has changed, says Mr. Ali. Anti-virus used to be a one-off installation, but now it is updated continuously because "it has been 'cloudified'," he says. The same will happen to firewalls and a host of other security devices. "You no longer have to manually configure each device. Now, like the anti-virus, they too can be updated across the board, using rules (or policies) that can be centrally pushed out."

Salman Ali
Principal, Arthur D. Little

As a result, just as desk-based security enforcers from an office may not make good mall security guards, the kind of people and techniques required for data security are changing, says Ali. "Static protection is no longer the modus operandi of the future. Emerging security is based on dynamic traffic analysis. We contextualise why someone is accessing a service, in effect applying a new type of filter." And these filters can be built, modified and torn down according to need-just as the cloud-based applications and virtual machines they are protecting.

> "Having an informational advantage in security brings many benefits"

FUTURE-READY PROFESSIONALS

"Tomorrow's security professional will be less of a compliance officer and more like a security technologist or even a security applications developer," says Mr. Ali.

The cloud is allowing and requiring a fundamental change in the way we approach security agrees Daniel Dalek, director of research and development at NTT Com Security in Gothenburg, Sweden.

"The pace of malware development has already reached levels where signature based approaches can no longer keep up. Combined with an exponential increase in data volume and complexity we need to think differently on how we can protect our customers," he says. Cloud offers many opportunities to do so, he adds.

"One of the major strengths of cloud based systems is providing reliable access to resources. Being able to scale out is also a strong security advantage where you are able to grow your environment in a flexible yet controlled manner." says Mr. Dalek.

NTT Com Security serves over 8,000 customers world-wide. The experience gained by supporting many clients also helps. "Having an informational advantage in security brings many benefits," he says. "Advanced analytics is often used as a trigger for incident response teams. Being able to identify attacks and compromised machines will allow an organization to take advantage of previous investments in incident response."

Daniel Dalek
Director of Research and Development, NTT Com Security

Despite the considerable challenges posed by cybercriminals, Mr. Dalek is optimistic about the future: "By focusing on behavior-based detection methodologies using machine learning (a subset of artificial intelligence or AI) we can provide more robust prevention capabilities. We strongly believe this will finally turn the tables and allow security vendors to be more proactive."

Peter Purton is a freelance writer, based in the UK