THE one BRIEF
AON EXPLORES THE WORLD'S MOST PRESSING BUSINESS ISSUES

RISK & INNOVATION

From Malware To Phishing: Your Guide To Cyber Crime

OVERVIEW

In May 2017, computer users around the world were greeted with a worrying red screen and a message demanding the payment of up to $600 in bitcoins to unlock their computers. This was "WannaCry", one of the biggest ransomware attacks in history. It is estimated to have caused around $4 billion in damages, hitting around 200,000 targets, including the U.K.'s National Health Service and Spanish telecoms provider Telefonica.

In Aon's 2017 Global Risk Management Survey, cyber risk was rated a top five global risk. In 2016, it cost the global economy an estimated $450 billion and resulted in around two billion stolen records – including over 100 million U.S. patient records. By 2019, losses could hit $2 trillion – more than two percent of the world's economy.

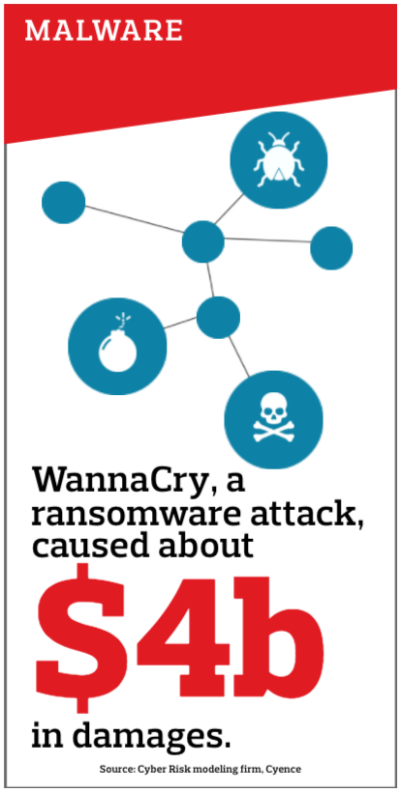
Companies, and their leaders, are aware of this. But while it's one thing to admit there's a threat – it's another to actually address it. And as our lives become increasingly digitized, the onus will be on us to understand exactly what types of cyber threats are out there.

IN DEPTH

Types Of Cyber Crime

Classifying cyber attacks isn't straightforward, as one attack will often combine several methods. For instance, a social engineering attack may result in a USB stick infected with a computer virus being connected to company systems.

Because cyber threats and methods can overlap and mesh together, the following categories may not always be completely cut and dried. However, they do give a good indicator of the range of attacks and hostile tactics that organizations have to deal with.



Malware

Malware is a term that covers a wide variety of computer viruses. Any malicious code that finds its way on to a system with the aim of impeding the operator's interests is classified under the malware umbrella. Adware, spyware, ransomware, worms, viruses and bots are all types of malware, and can all make their way into a network in a variety of ways.

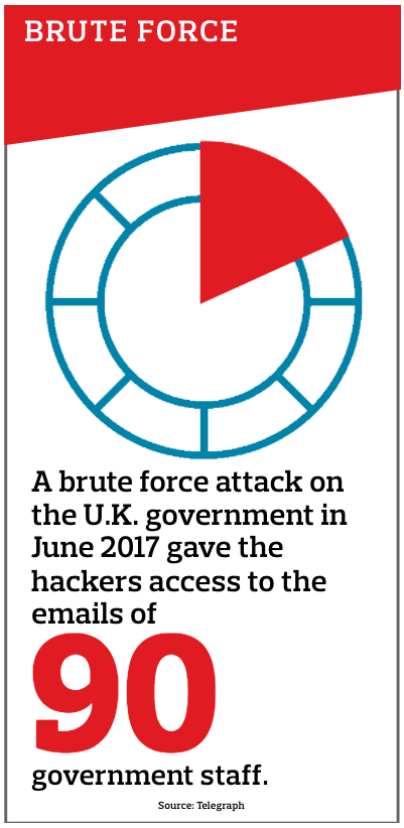
Malware can cause damage in various ways, including shutting down computer systems until a ransom is paid, or destroying operational systems. Malware attacks are one of the fastest-growing areas of cyber crime, with a sharp jump in the number of organizations affected – the number of ransomware attacks alone increasing 167 times year-on-year from 2015 to 2016.

DoS

A Denial of Service (DoS) attack occurs when an attacker overloads a network with excess traffic, causing that system to shut down.

One particularly prominent trend is the Distributed Denial of Service (DDoS) attack, when a multitude of different viruses all visit a network at once – making it impossible for the victim to manage the attack by simply blocking individual users. In late 2016, a DDoS attack took down a significant portion of the internet, including Netflix, CNN and Reddit.

Financial gain isn't always the motivation behind DoS attacks – they could be launched to disrupt or sabotage operations or cause significant business interruption. The average DDoS attack costs a business around $2.5 million.



Brute Force Attacks

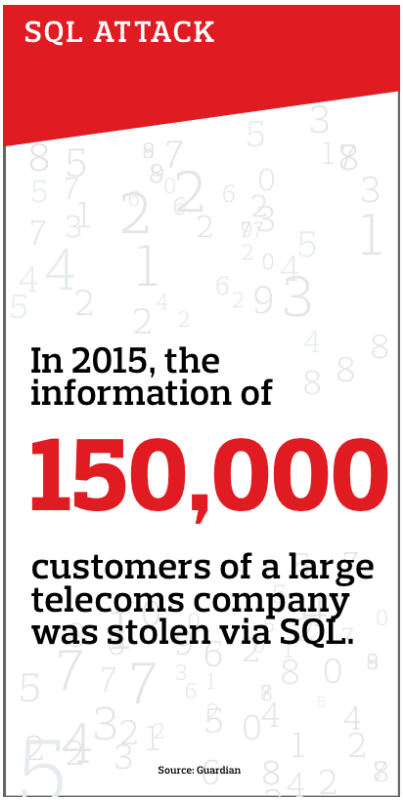
Brute force attacks try to guess a system's passwords by running through every combination of characters at high speed, usually in an effort to uncover sensitive information. Varieties include dictionary attacks, where algorithms run through known words or character combinations in the hopes of hitting a correct combination.

A brute force attack on the U.K. government in June 2017 gave hackers access to the emails of 90 government staff – potentially including lawmakers and even the British Prime Minister.

SQL Injection

SQL (pronounced "sequel") stands for Structured Query Language, a computer language used to communicate and issue instructions to digital databases. SQL attacks involve directly injecting malicious code into websites, which then exploits vulnerabilities in their databases so a hacker can access and tamper with records.

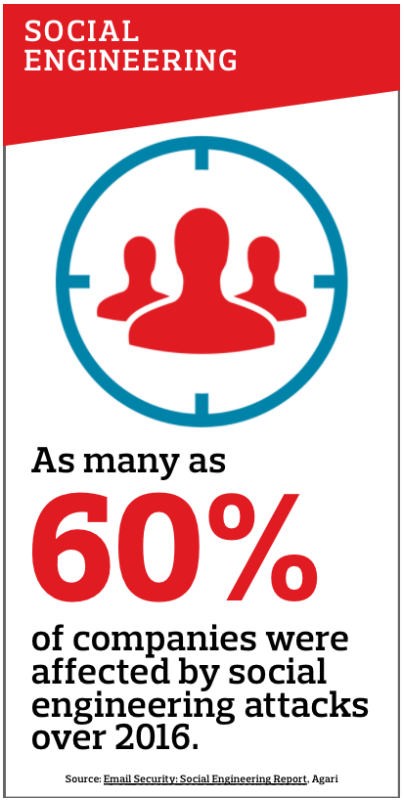
By issuing fraudulent instructions, attacks can manipulate those databases and the assets they contain, which can pose a significant risk to both businesses and their customers. For instance, a SQL injection could be used to extract card details from retailers' databases. In 2015, the details of 150,000 customers of U.K. telecoms group TalkTalk were stolen via SQL injection attack.



Phishing

Phishing is the attempt to access or manipulate a target network, by posing as something more innocent. For example, a target might be sent an email purporting to be from a trusted contact or colleague that contains a link that, when clicked, downloads malware onto the user's computer.

Despite widespread campaigns to encourage better awareness of phishing, research shows that as many as one in three phishing emails get opened.



Social Engineering

Related to phishing, but more sophisticated, is social engineering. Here, instead of pursuing targets over digital channels, the attacker appeals directly to the person at the other end, via a phone call or face-to-face, using psychological tricks and intimidation.

The famous "Nigerian Prince" email is an example of "spear-phishing" – an email-based social engineering attack intended to open up a direct channel of communication to an individual, before using traditional con-artist tricks to gain access to money or sensitive information. Today, attackers are getting more sophisticated and targeted – for instance, a target might receive an email or a phone call from someone pretending to be a senior executive demanding valuable account information.

As many as 60 percent of companies were affected by social engineering attacks in 2016. And recently, even the White House fell victim to an email scam.

3 Ways To Boost Your Cyber-Resilience

Cyber attacks are almost inevitable. The risk profile is substantial, and it's unlikely that any organization can fully shield itself from incidents with technologies and techniques changing so rapidly.

1. **Employ best-in-class cyber security technology standards:** It sounds basic, but making sure your technology profile is up to date is a key step in limiting exposure to cyber crime. Installing relevant anti-virus software should be standard business practice. But organizations must also remember to keep existing technology up to date. The WannaCry attack particularly affected computers running out-of-date, unpatched software.
2. **Manage your people risk:** Up-to-date technology is critical, but it can all be for nothing if companies fail to recognize and control the risk posed by their people. People can make mistakes, fall prey to social engineering attacks, or simply act out of malice. More often than not, it's human error that lies at the heart of major security breaches. Educating your staff on their responsibilities, and on the dangers they face is key.
3. **Establish response strategies:** Even the most cautious firm which follows all the best cyber security practices may still become a victim of a cyber attack. Having a plan in place to manage attacks when they happen is therefore crucial. Do key stakeholders know what they should do when an attack happens? Are there steps in place to incubate or control the spread of malware? Establishing and testing response strategies, through red-teaming or tabletop exercises, can help close these gaps and ensure that a company is prepared for an attack when one happens.

Vigilance is essential. Some cyber attack methods are well-established, relatively easy to protect against – and yet still prove successful. Failure to adequately protect your operations may even impact your ability to get insurance to reduce the impact of a breach when it occurs. Increasingly, failing to keep up with the basics of cyber-resilience will prove a significant business threat – not just in terms of monetary impact, but also in terms of reputation and long-term business viability.

"We live in a continually evolving digital and technology inter-connected environment, where companies face challenges keeping up with the latest security solutions – this leaves them more exposed to potential cyber attacks and related threats than ever before," says Aon Inpoint CEO, Michael Moran. "At some point, even the most sophisticated system will likely be breached, as new technologies and techniques emerge."

TALKING POINTS

"The first thing is to get away from the perception that cyber is just a technology problem that can be solved entirely through engineering solutions. There is a tendency for boards to look at it, fear that it's too technical to understand, and then delegate the whole issue to technologists – who duly deliver some technological fixes. The trouble with that is that most cyber attacks are not exclusively – or even mainly – technical in nature. People and processes are every bit as important." – Will Brandon, Chief Information Security Officer, Bank of England

"An attack might come from a hacker for political goals. Or one with financial motives. It might be a threat made through ransomware, a hybrid threat or even nation-state cyber-espionage. Or it might have no obvious objective other than to 'disrupt' for the sake of it. The definitions are not as clear as before... The concept of a predictable threat – as we used to know it – is long gone. Today, both the targets and the attack methods are far more unpredictable." – Andrus Ansip, European Commissioner for the Digital Single Market and Vice President of the European Commission

FURTHER READING

- Cyber Attacks Were On The Rise, Even Before The Latest Episode – The Economist, May 15, 2017
- The New Cyber Risk Requirements – CIO, July 6, 2017
- Companies See The Cyber Threat, But Spending On Security Is A Different Matter – Financial Post, May 30, 2017
- Insurers May Have To Adjust Policies To Reflect "Silent" Cyber Risks – The Register, July 11, 2017
- Beware Of these Top 10 Phishing Emails – Fortune, July 13, 2017