CHUBB®

The Frontiers of Technology Risk

Cyber Risk Awareness for IT Companies

CHUBB®

Cyber Risk Awareness for IT Companies

Contributors

Barry Schütte
Manager Industry Practices Benelux, Chubb

Wouter Wissink
Senior Principal Cyber Risk Engineer and Technology Industry Practitioner, Chubb

Cyber security is a risk area that requires a monumental focus, particularly with global cyber crime costs predicted to reach around $10.5 trillion annually by 2025, according to Cybersecurity Ventures. IT companies are especially vulnerable to hackers, with their role as intermediaries making them a target to distribute malware or ransomware to multiple businesses in one event.

The Kaseya and SolarWinds attacks are two high profile examples of the damage that can be caused by ever more sophisticated criminal enterprises. Organised hackers are increasingly motivated by monetisation of their activities, with ransomware now the biggest cyber threat, the European Union Agency for CyberSecurity warns.

Stopping cyber crime requires robust security and continuous attention to controls. Risks can be significantly mitigated by complying with certain cyber hygiene measures. But with attacks becoming progressively targeted and advanced, what should IT companies be doing to protect themselves?

Common exposures

These companies face two basic risks that are very much connected: attacks on their own environments and those causing harm to customers. A cyber hack on a software developer or distributor could lead to theft of confidential data, which might then be misused by hackers to directly access a customer environment. If a technology company is attacked by ransomware, it may be unable to provide core support desk services to clients. Or software compromised by backdoor malware can get unwittingly sold to customers, facilitating an attack on hundreds or thousands of businesses.

Cyber criminals are also capable of inflicting damage by gaining access to clients through Managed Service Providers (MSPs), warns Wouter Wissink, Senior Principal Cyber Risk Engineer and Technology Industry Practitioner, Chubb.

The business, financial and reputational repercussions for IT companies can be huge, says Barry Schütte, Industry Practices Manager, Chubb. “Worried companies may move to a competitor, for example, which impacts the bottom line,” he explains.

Tough business decisions

What can be learnt from the Kaseya and SolarWinds crises? In the case of US multinational Kaseya, in July 2021, vulnerabilities in its Virtual System Administrator (VSA) software – supplied to MSPs and IT teams – were exploited by hackers in a zero-day attack.

Cyber hygiene best practice checklist

- Can you identify the risks your company and customers face?
- Do you know what to do to prevent these exposures?
- Are there robust measures in place to detect cyber risk?
- Is there a clear plan for how to respond if you are hacked?

"As the 'man in the middle', MSPs face real cyber risk"

"This in-between period is very difficult to protect," explains Wissink. "Software companies need a week or longer to fix this kind of issue and during this time these developers are very exposed."

The Kaseya loss was limited to around 50 clients, but up to 1500 downstream companies worldwide were allegedly also hit by ransomware.

Exposure to these kinds of attacks is accelerating. In 2021, zero-day exploits were reported to have doubled, according to a report by Rapid7. "This is the most critical risk area because it is very difficult to manage," says Wissink. He urges affected companies to inform clients on the same day a system is hacked, swiftly take systems offline and keep customers updated.

"That can be very difficult for some companies," he cautions. "You are essentially telling clients your business model is no longer safe and they need to go offline."

Backdoor tactics

Six months before the Kaseya incident came the so-called Solarigate supply chain hack, in which cyber criminals added malware to updates in the SolarWinds Orion software system – widely used by companies managing IT resources.

"Hackers were able to gain access to the development environment," says Wissink. The malware spread undetected as part of a regular software update for clients, creating a backdoor to their IT systems. Around 18,000 customers were exposed, including US government agencies and global brands. According to Wissink, "basic cyber hygiene measures could have prevented this attack".

Emerging trends

What trends are insurers seeing these days? Companies are improving their own protection levels, says Schütte, so cyber criminals are increasingly targeting vendors and suppliers. As the 'man in the middle', MSPs face real cyber risk, and the steady growth in this market has been accompanied by a rise in claims.

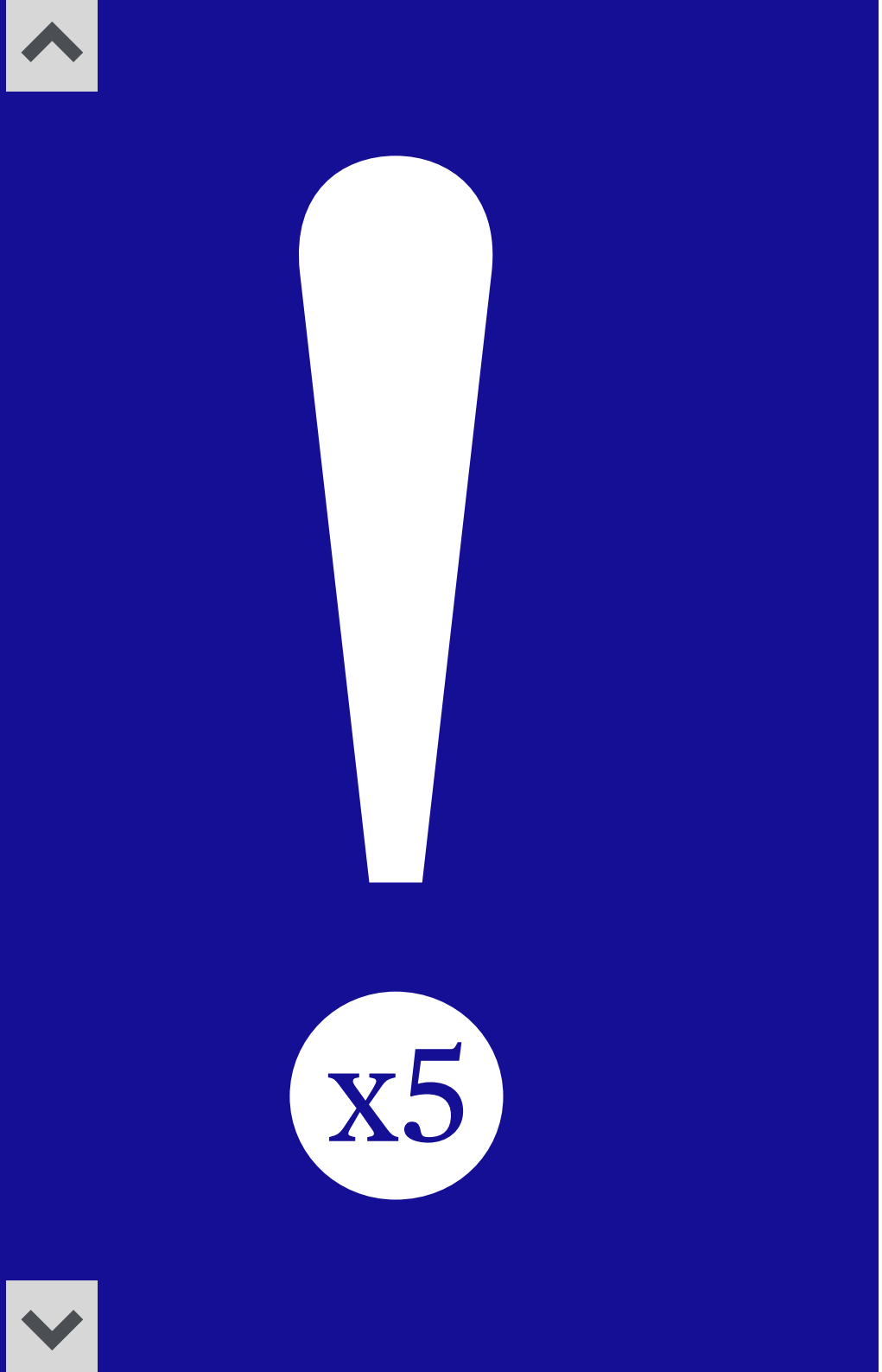
"Platform as a Service (PaaS) and Software as a Service (SaaS) are also more exposed," he adds. "So the risk profile has significantly increased with this shift away from on-premise software systems to platform or cloud-based business models."

Duty of care is another emerging risk area. In a supplier/client relationship, an IT company is generally considered the expert, explains Schütte. "Its responsibilities often go beyond what is written in an agreement, which means the liability risks escalate." One provider advised a client to take extra security measures but failed to document the advice. When the customer experienced a ransomware attack and later sued, the IT company was found liable.

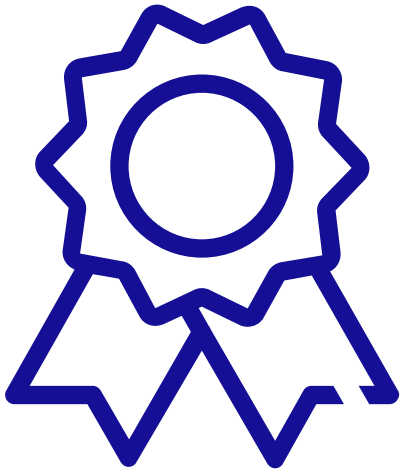
So how can these risks be mitigated through good cyber hygiene? We look at best practice for IT companies around four key strands: identify, prevent, detect and respond.

Pinpointing the risks

Establishing cyber-related risk is just a question of robust risk management, say Wissink and Schütte. IT companies must identify exactly what products and services they provide to estimate what can potentially lead to risk. Do they make software? Do they distribute software? Are they an MSP? Do they store passwords for clients?



"Instead of one major risk, we are now seeing five major exposures, so the risk for IT companies is five times higher than it was 10 to 15 years ago"



An Information Security Management System (ISMS) allows companies to determine these details. This centrally managed framework enables them to manage, monitor and review their information security practices.

While software developers generally devote "a lot of effort" to creating a secure product, Wissink says similar safeguarding for their own environments is often missing. For example, clients are regularly asked to download the software from a website that is not well protected.

Fortifying the defences

Stopping cyber attacks requires, at the very least, standard hygiene measures, including multi-factor authentication, adequate awareness training for staff, firewalls, scanning phishing emails, and filtering websites.

"But IT companies really should have the absolute best practices in place, given the greater potential impact of losses from a widespread event and increased duty of care responsibilities," advises Wissink. He says companies need a Privileged Access Management (PAM) system. The PAM tool preserves identities, with special access or capabilities beyond those of regular users. It is particularly important for MSPs, which have many people accessing multiple programs through a central software package.

Software development companies must also segregate their network and safeguard it with additional tools only developers have access to, urges Wissink. "This development environment should not have an auto connection to the rest of the company."

Other good housekeeping measures to reduce exposure and help with business continuity include continually testing backups and storing these offline and a razor-sharp focus on encryption for passwords and other data. Hiring a dedicated IT security officer is a smart move, too.

"Companies must protect this data but should also have a good contractual agreement with the customer on how to store and process their data," says Schütte.

But prevention is not only about technical prevention measures. It is about communication –contractual service level agreements and data protection agreements. "An IT company, and especially an MSP, has a duty of care to warn and instruct customers about the potentially poor protection level of a specific client environment," adds Wissink. "Customers should be informed in writing, and to protect liability, this should also be documented."

According to Schütte, many IT companies are behind in evolving secure development policies. This includes penetration and vulnerability testing, as well as code review and training in writing code (OWASP Top Ten can help).

Software developers that create non-critical software should not ignore the need for these policies, he advises.

"In today's threat landscape, every company is a target," warns Wissink.

Key takeaways

- **Attacks on MSPs are the biggest** emerging claims trend
- **IT companies need a better handle on** zero-day exploits
- **Duty of care risks are rising and** should be on companies' radars
- **An Information Security Management System** (ISMS) can help to identify risk
- **Use a PAM (Privileged Access Management)** tool to help stop hackers
- **Segregate your software system from** the rest of the company
- **Communication with customers is** also key to cyber prevention
- **Implement adequate secure** development policies
- **A network monitoring system** (tracked 24/7) is a wise idea
- **Do not ignore formal incident response** and business contingency plans
- **Remember to continually test backups** and store these offline

Detecting cyber breaches

Monitoring software and detection software, such as EDR (Endpoint Detection and Response), are a must for IT companies. As are satisfactory firewalls or a network monitoring system, tracked 24/7 by an internal or external security operations centre. "Once a hacker gets into a system, it is vital they are detected in time," stresses Wissink.

Putting out the fire

Both Wissink and Schütte agree that one of the most business-critical elements for dealing with cyber attacks is a clear incident response plan. Thorough advance planning will help a company react appropriately and quickly if they have been hacked. For a software company, this plan goes beyond their own IT environment and should also include a client communication and crisis management policy. In their experience, many companies are not prepared. "Much of the time, they do not know what to do," says Schütte.

If IT systems are violated, companies must ensure services are secure and back on track as soon as is viable, and that they are able to serve customers competently in the intervening period.

The future of cyber-related risk in the digital era may seem daunting, but failing to take preventive steps to protect your business is a bit like permanently leaving the front door wide open and hoping nothing gets stolen. It makes much better business sense to educate yourself about cyber hygiene and put the appropriate elements in place to protect yourselves and your customers.

Key contacts

Barry Schütte
Manager Industry Practices Benelux, Chubb
bschutte@chubb.com

Wouter Wissink
Senior Principal Cyber Risk Engineer and Technology Industry Practitioner, Chubb
wwissink@chubb.com

Chubb. Insured.℠

All content in this material is for general information purposes only. It does not constitute personal advice or a recommendation to any individual or business of any product or service. Please refer to the policy documentation issued for full terms and conditions of coverage.
Chubb European Group SE (CEG). Operating in the UK through a branch based at 100 Leadenhall Street, London EC3A 3BP. Risks falling within the European Economic Area are underwritten by CEG which is governed by the provisions of the French insurance code. Registered company number: 450 327 374 RCS Nanterre. Registered office: La Tour Carpe Diem, 31 Place des Corolles, Esplanade Nord, 92400 Courbevoie, France. Fully paid share capital of €896,176,662.

UK8208-WA06/22