THE GLOBE AND MAIL

OPINION

Online crime presents new challenges for insurers

CHRIS MCKIBBIN
CONTRIBUTED TO THE GLOBE AND MAIL
16 HOURS AGOSEPTEMBER 5, 2017

Chris McKibbin is a partner, Insurance Practice, at Blaney McMurtry LLP in Toronto.

Any business in its right mind has crime insurance. What it may not have is the protection it needs to face new threats such as social-engineering fraud and ransomware.

The recent $11.8-million vendor-impersonation scam against MacEwan University in Edmonton is only the latest high-profile social-engineering fraud in what has become a multibillion-dollar criminal industry.

So where does crime insurance come in? All too often, it doesn't – and it's not supposed to. Historically, crime insurance, also known as fidelity insurance, has been geared toward tangible risks such as employee embezzlement, loss of money in transit and computer fraud (hacking an insured's computer to illicitly transfer funds without the insured's knowledge). New types of fraud, such as social-engineering fraud and ransomware, do not fit into these neat categories. Canadian and U.S. courts have generally held that social-engineering fraud losses are not covered under crime policies. This has led some businesses to feel not only victimized by the fraudster, but also disappointed with their insurance broker or adviser for not ensuring that appropriate coverage was in place.

Business losses from social engineering fraud have been staggering. In May, 2017, the FBI reported that business e-mail compromise scams had grown 2,370 per cent in the previous two years and had resulted in more than $5.3-billion (U.S.) in losses since 2013. Unfortunately, business e-mail compromise scams are but one form of social-engineering fraud, a catch-all term encompassing frauds that share a common characteristic: All include a fraudulent act inducing an employee to voluntarily part with the assets of the business. Three of the most common forms of social-engineering fraud are:

- Vendor impersonation: The fraudster poses as a legitimate vendor of the target business and contacts the target's employee to update the vendor's banking information, either by using an imitative "spoof" e-mail or by compromising the legitimate vendor's actual business e-mail account. The target unwittingly wires funds to the "new" account, which is in fact controlled by the fraudster.
- Executive impersonation: The fraudster, posing as the target's CEO or other high-ranking executive, contacts the target's finance department using a spoof or compromised e-mail, under the pretext of needing an urgent payment relating to a "secret" acquisition, merger or settlement. The fraudster directs the employee to wire funds to a "special" account, controlled by the fraudster.
- Client impersonation: The targets of these scams are financial institutions or other entities that handle client funds. The fraudster poses as a legitimate client and uses e-mail, phone or fax communications to induce the target to wire the client's funds to a "new" account controlled by the fraudster.

Fortunately, Canadian insurers have introduced optional social-engineering-fraud coverage as extensions of their crime-insurance offerings over the past few years. Nevertheless, insurers continue to see claims submitted under policies lacking this coverage.

Ransomware is in a separate category. It is malicious software designed to encrypt the target's computer files and to block access to the target's system until a ransom is paid. In May, 2017, the notorious WannaCry attack hit more than 230,000 computers in more than 150 countries.

Although most attacks have sought relatively small amounts from targets, the ransom payment is usually only a fraction of the total cost of a ransomware attack. Remarkably, within the first 72 hours of the WannaCry attack, the total ransom paid was only about $20,000; the resulting economic loss, however, has been estimated at as high as $4-billion, comprised of lost productivity, forensic-investigation expenses and data-restoration costs.

To address the ransomware threat, some Canadian insurers are now offering cyberrisk policies that include cyberextortion coverage. But even cyberrisk policies may be limited in scope, excluding such categories as loss of productivity.

Crime policies will not ordinarily respond to either the direct or indirect costs associated with a ransomware attack, as such attacks do not meet policies' definitions of computer fraud. Many crime policies also contain specific exclusions that encompass ransomware losses. Crime insurance and cyberrisk insurance are distinct coverages and are intended to cover distinct risks. Canadian insurers are moving to meet market demand for social engineering and cybersphere risks. But it's still up to businesses and their insurance brokers to make sure that the appropriate coverages are in place.

References

https://beta.theglobeandmail.com/report-on-business/rob-commentary/online-crime-presents-new-challenges-for-insurers/article36171381/?ref=http://www.theglobeandmail.com&