DENTONS RODYK

Corporate response playbook if a company becomes a victim of a scam or cyber-attack

Scammed or hacked?
Overview of common fraud techniques and the corporate response playbook

Nobody is immune to scams and cyber-attacks. With the increase in scammers' levels of sophistication, their targets have also increased in scale. Scammers even routinely target multinational corporates and banks which have far more robust defences and highly trained personnel than the average SME.

Victims of scams and cyber-attacks face numerous consequences, including the difficulty of trying to unravel fraudulent transactions, exfiltration of sensitive financial or personal data, and disruption of key IT services. Some recent examples include the following:;

- In March 2021, a local furniture retailer was hacked, causing the phone numbers and physical addresses of its customers to be leaked online. The hacker group claimed that it had hacked into the company's database and stolen information related to more than 30,000 customers and nearly 600,000 transaction records.
- In May 2021, it was reported that an employee of a local bank allegedly fell prey to an impersonation scam that caused the leak of the names, identification and mobile numbers and account balances of over 1,100 customers of the bank. The employee had allegedly fallen victim to a Chinese police impersonation scam and was duped into disclosing the information of customers from China with Singapore-based accounts.

Apart from the direct consequences of cyber-attacks/scams, a whole range of questions that senior management and directors of affected companies must answer will swiftly arise such as how do we determine who is responsible and what went wrong? Or how the matter should be reported to the authorities and how should it be communicated to clients and/or shareholders? Is it be possible to retrieve the funds in the hands of the fraudsters? What should be done first?

This article seeks to set out a brief overview of common scam techniques and provides guidance on the consequences/potential liabilities that may arise, and more importantly, what should be done in the event of a scam being perpetrated on corporates.

Common Scam Techniques

i. Business Email Compromise (BEC) scams

In BEC scams, fraudsters approach employees of companies, passing themselves off as a known vendor or client of the company. Such fraudsters commonly hack/takeover the email accounts of the vendor, or impersonate the vendor by creating a similar looking email. Fraudsters may also attempt to pass off as CEOs or Senior Executives in order to request for sensitive data, often with a view to using such data in subsequent attacks such as to bypass security verification/authentication tools.

ii. Fake invoice scams

Another common scam is to utilise fake invoices, wherein fraudsters posing as known vendors generate fake/modified invoices using legitimate billing information or upcoming invoice, but with modified payment details that will route the payment to the fraudster's bank account instead.

iii. Ransomware

Getting users to click links in a phishing email, pop-up windows from a suspicious websites, and emails requesting one to download attachment are common ways of tricking employees into installing malicious software on their workplace computers. This may grant fraudsters the ability to steal the company's data and to remotely lock your files and prevent access unless a ransom is paid.

Potential repercussions of scams/ cyber-attacks

The consequences for victims of scams/cyber-attacks are myriad and multifaceted. Anyone and everyone in the company's chain of command as well as clients and potential clients may be affected. Corporate entities who fail to secure the personal or financial data of their customers face not only reputational risks, but may also be found to be directly liable to the affected customers, not to mention potential breaches of regulations relating to, amongst others, cybersecurity and data privacy. Questions on breach of confidentiality obligations or fiduciary duties may also arise.

i. Direct consequences

Fraudulent transmittals of funds to scammers, and having to pay a ransom to regain control of critical IT systems/data would obviously cause losses and operational disruptions. The company may even to pay damages or fines. A company's intellectual property such as its know-how, technology, designs, and trade secrets could also be stolen and are vulnerable to cyber-attacks especially if stored on the cloud/third party servers.

Clients entrust personal information into the hands of the company on the basis that it is well stewarded and where their personal information has been leaked, a company has a duty to notify the authorities and/or the individuals affected (sections 26A – 26C of the Personal Data Protection Act (PDPA)). A person who suffers loss or damage directly as a result of data breaches may also have a right of action for relief in civil proceedings in court (section 48O, PDPA). On that note, although difficult to quantify, companies that fall victim to large cyber-attacks will invariably face reputational damage. Customers and suppliers may feel less confident in sharing their sensitive data/information with a company that has already been scammed or hacked once.

A notable example: in September 2017, a company (an American multinational) involved in consumer credit reporting business announced a data breach that exposed the personal information of 147 million people. The company subsequently agreed to a global settlement with the U.S. Federal Trade Commission, the Consumer Financial Protection Bureau, and 50 U.S. states and territories. The settlement included up to $425 million to help people affected by the data breach.

ii. Investigations, other indirect consequences and individual employee liability

The affected organisation may also face increased costs in having to hire experts to prevent repeats, to investigate the incident, and having to conduct additional security/compliance training for its personnel. Precious man-hours may also have to be spent on cooperating with the authorities for investigative purposes instead of being spent on the company's core functions.

Within the organisation itself, there would inevitably be a need to determine what went wrong, and whether any individuals are at fault, and if so whether any disciplinary sanctions are merited. It is not uncommon for there to be a breakdown in the relationship between employer and the individual employee found to be at fault. This can result in the employee leaving the company – either by agreement with a clean break. If the individual employee is found to be at fault, for example by failing to follow company protocols or policies, the employee may be terminated for cause as the employment contract may provide. The company should be careful to conduct a proper internal investigation (as elaborated on below) to avoid incurring any potential liability for wrongful termination. These would all result in increased costs for the company, whether in terms of investigative costs or in having to replace employees.

While it is settled law that employers are vicariously responsible for the harm caused by an employee in the performance of his duties (see section 53 of the PDPA which provides that any act done or conduct engaged in by a person in the course of his employment shall for the purposes of the PDPA by deemed to have been as done or engaged in by his employer whether or with the employer's knowledge/approval), there may arise a question of whether the employer can pursue a claim against the individual employee responsible for the data breach/fraudulent transmission. Deciding whether there are any merits and if it is worthwhile for the employer to pursue such a course of action is another issue that the affected company may have to consider.

Prevention is better than a cure

Employees may become the biggest weak spot in the ongoing battle against scammers and fraudsters. As compared to sophisticated cyber-attacks or hacking, it is more cost-efficient for fraudsters and often easier to try to utilise social-engineering techniques on employees into disclosing sensitive data or making fraudulent fund transfers. Therefore, it is important to ensure that employees are adequately trained to deal with situations involving scammers/common fraud techniques. This is key not only for employees involved in finance roles/data management, but for all employees of the firm. Refresher training should be conducted on a regular basis.

Whilst the employees are the 'software' and 'brains' of an organisation, the organisation must at the same time invest in its 'hardware' to keep itself secure from threats emanating from the cyberspace environment. It is vital that companies incorporate anti-virus/anti-malware software, and other digital authentication tools to mitigate risks such as customer fraud and identity theft. Security monitoring and web isolation are also useful tools.

Auditing the company's processes should also be part of consistent ongoing efforts. This can include conducting regular vulnerability assessments:
(i) on IT systems to identify any security vulnerabilities to ensure gaps can be plugged in timely manner;
(ii) drafting/reviewing of pre-determined plans or courses of action to implement upon the occurrence of certain pre-identified risks or incidents.

The Quick Response Playbook

The most critical thing for the company to do is to establish a systematic plan from the outset. This will serve to identify the key issues to be dealt with, assist with budgeting, and help to avoid pitfalls which may prejudice the company's position further down the line.

While each incident and organisation will have its own specific concerns, the following steps serve as a basic framework.

1. Incident identification
2. Triage and assessment
3. Implementing the plan of action, including conducting internal investigations
4. Resolution & Remedial actions

1. Incident Identification

The very first step is to quickly identify what has happened by compiling the fundamental information pertaining to the incident:

a. Nature of the incident

b. Whether there is any basis to the allegations made

c. Personnel involved

d. Preliminary assessment of risks involved

e. Preliminary assessment of urgency/priority to be accorded

f. Informing key advisors in the Company (i.e. legal, PR etc) so that parties are aware of what is going on.

This is not meant to be a comprehensive fact-finding exercise, nor should this be treated as an opportunity to ascertain who is at fault at this stage. The purpose of the exercise is simply to gather enough information to enable the company's management/board to make an assessment of what to do next.

2. Triage and assessment

As the name suggests, the next step 'triage' is the process of determining the extent to which the company's resources ought to be brought to bear on the incident/allegation. It is to carry out an early assessment of any allegations, and to compel the decision makers to think through the correct investigative approach to be adopted.

Principle considerations would include:

a. Risk categorisation – high risk allegations such as misappropriation of company funds/corruption by senior management, or lower risk incidents such as breaches of internal protocol.

b. Significance or scale of the incident/allegation – one-off incident or whether there is a suggestion of recurring breaches

c. Whether the incident/allegation, if true, exposes the company to financial impact, legal liability and/or reputational risk

d. Seniority of personnel involved – whether senior management team is involved which may cause a crisis of confidence in the operation of the business

It is at this stage, where the board/management should decide what kind of resources are required. For example, if it is a low impact incident such as access to illicit sites, perhaps all that would be warranted would be a routine internal investigation. On the other hand, if the preliminary assessment reveals a high impact incident (leakage of customers' personal/financial data, theft of intellectual property, ransomware, unauthorised/fraudulent fund transfers), the management team should then consider bringing formally engaging external advisers such as legal counsel, investigative experts, forensic experts, public relations team etc.

It is also appropriate at this stage, depending on the seriousness of the incident, to consider bringing on board external advisers (such as lawyers, forensic investigators, technical experts, accountants)– not necessarily to immediately commence substantive works – but rather to provide the management team with an overview of the scope of work/issues that need to be addressed. Such an approach, would help keep investigative costs lower and help the company to make an informed decision on how to allocate its resources whilst working on mitigating any damage.

In short, the triage/assessment stage involves working toward preparing a specific and deliberate plan of action.

3. Implementing the plan of action, including conducting internal investigations

The plan formulated by the management team with the assistance of its advisers should cover all relevant issues, in particular the following key issues:

a. Immediate actions:

i. Identifying root cause of scam, security breach / data loss, isolating comprised system to prevent spread of virus/malware, remedial actions to eradicate malware/ransomware

ii. Dealing with adverse publicity and writing press releases

iii. Disclosure/self-reporting obligations. For instance whether the incident triggers self-reporting obligations under anti-money laundering legislation such as the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act, or under mandatory notices issued by the Monetary Authority of Singapore. Companies Listed on the Singapore Exchange may have obligations under the Listing Manual to make certain disclosures.

iv. Consideration of whether to lodge a report with the authorities

v. Whether there are any immediate steps that need to be taken to try to recover monies paid out as a result of the scam or fraudulent transaction

b. Typical internal investigations involve conducting interviews with relevant employees, management/directors, collection and forensic review of records, as well as tracing the proceeds of fraud monies (possibly even applying to Court for injunctions or freezing of assets). Conducting such internal investigations necessarily involves consideration of a wide range of issues:

i. Protocol for investigation – consideration of scope of protection afforded by legal/litigation privilege to records created in the course of investigation is of paramount importance.

ii. Cross-border considerations – extent of legal protection/privilege of documents differs from jurisdiction to jurisdiction and it is critical to establish such differences at the outset. Other consideration could include what kind of material can be seized and relied on by authorities, whether there is a privilege against self-incrimination

iii. Restricting circulation of investigative records/ materials to only specific stakeholders

iv. Scope of investigation – whether criminal, regulatory and/or civil litigation is anticipated

v. Evidence gathering and fact finding process – whether to be delegated to external counsel and/or conducted by in-house counsel

vi. Scope of investigative report – identifying cause of the incident, potential exposures, advice on next steps/remedial actions to be undertaken

c. Cooperation with authorities/regulators

i. Any plan of action should also take into account the possibility that the matter may be investigated by the authorities/regulators.

ii. Advice should be sought on whether to waive privilege and turn over material to the authorities, on the basis that voluntary cooperation would be favourably regarded or viewed as a mitigating factor

iii. In terms of enforcement proceedings, the organisation also ought to consider whether it will be held liable for its employee's conduct or whether it is entitled to disclaim responsibility

4. Resolution & Remedial actions

This stage largely involves preparing material for the purposes of regulatory reporting, insurance claims, civil litigation, disciplinary actions against employees concerned, and other issues such as customer notification and management of public relations issues. Needless to say, it is also important for management to implement the lessons learned to prevent a repeat of the situation and to improve defences.

Conclusion

Despite best efforts, it is not always possible to prevent falling prey to scams and cyber-attacks. However, preventive measures to reduce instances of such conduct can and should be implemented. More importantly, once an incident has occurred it is important to take all necessary measures to mitigate potential liabilities and to ensure that the least possible amount of damage is sustained.

Getting external counsel and advisers in at an early stage to advise on a concrete plan of action does not equate to ridiculous expenses or fees incurred. Fee agreements can be reached on a phased basis to first ascertain the necessary scope of work and to provide a preliminary assessment of the potential issues involved, before any decision is made on the substantive scope of work to be undertaken by the external advisers.

On the contrary, proceeding without any concrete plan of action may result in poor process management and unnecessary complications further down the line. For instance, many an organisation has proceeded to conduct its own internal investigations without adopting a considered approach to legal/ litigation privilege, only to later find out to its chagrin that its internal records are not protected by privilege and have to be disclosed in civil proceedings and/or to the authorities.

We hope this article provides some guidance on responding to such events and our firm would be pleased to assist or discuss next steps on any such matters.

Contacts

Ajinderpal Singh
Senior Partner
D +65 6885 3619
ajinderpal.singh@dentons.com

Sunil Rai
Partner
D +65 6885 3624
sunil.rai@dentons.com

Jonathan Lim
Partner
D +65 6885 3729
jonathan.lim@dentons.com

ABOUT DENTONS

Dentons is the world's largest law firm, connecting top-tier talent to the world's challenges and opportunities with 20,000 professionals including 12,000 lawyers, in more than 200 locations, in more than 80 countries. Dentons' polycentric and purpose-driven approach, commitment to inclusion and diversity, and award-winning client service challenge the status quo to advance client interests.

dentons.com

CSBrand-64052-Corporate response playbook_02 — 19/07/2021