Sleight of hand in the digital age

Data manipulation affects industries from banking to manufacturing and is far more difficult to detect than simple data theft. This article explains how damage to digital assets can cost you dearly.

So you think you've covered your tracks to stop your data from being stolen. But have you ensured that it can't be manipulated in situ?

Data manipulation is exactly as it sounds, it's bad guys going into an environment and changing something to their benefit. Generally speaking, data manipulation is preferred over data theft because it's less easily detectable. For example, if you've got good security on board, you're going to notice if your data is being taken outside. But if someone gets into an environment and changes things, then this is much less likely to be discovered. It is common for hackers to protect themselves from being noticed during a data theft, so if I was to access your server and steal stuff out of it, it leaves log data. I'd want to delete that so there's no record of who or what has been there.

Banks are frequently hit by data manipulation. For example, thieves steal a cash card with a limit of £500. They then hack into the back-end database and increase the limit on the stolen cash card to £10,000. They then take the card and withdraw the full amount. This is more sophisticated than the tried-and-tested phishing emails which state "I've changed my bank details, please redirect all new payments here" method. What's becoming more common are hackers breaking into company accounts systems and changing bank details within.

Data manipulation by hackers is a particular problem in manufacturing, says Laurance Dine, Managing Principal at Verizon Enterprise Solutions "Often hackers will steal the master drawing, alter it and then create the product themselves while the original company has to start over and correct the mistake. This might be something as simple as a piece of glass that fits into an aeroplane." Manipulation of this kind is seen in state hacking scenarios or situations where big organisations want access to a particular marketplace.

So what should companies be doing to prevent data manipulation? "The key things we talk about are encryption and multi-factor authentication," says Dine, "so that's where the people that need to have access to data can't just use a password. There are very simple check-in and check-out pieces of software that will audit and log every person who's touched something." He adds, "Of course, that doesn't stop me from hacking your computer but if it's a master document or database that has high value to an organisation, using text-message authentication or biometrics would solve a lot of problems."

Segregation of data is crucial, too. Says Dine, "Only give people access to data that they need access to. We respond to incidents all the time where everyone has access to the file server. If this stuff is your crown jewels, then you need to make sure it's located somewhere else and only the people who need access to it have access." Moreover, he adds, "you need an audit of whatever they've done. If something is happening when it shouldn't be, then you need a notification. If a document is being altered at 2am when the rest of the time that document has been altered is between 9 and 5 on a weekday, someone needs to know it's been altered out of hours and by whom."

The GDPR (General Data Protection Regulation), which comes into effect in May 2018, will have an impact on data security. Whilst it's not possible to protect every file and every document you own in all these stringent manners, having data owners is very relevant and will make it more regulated, if not easier. The GDPR will at least ensure that somebody is in control of data.

Within the insurance landscape there's cover within cyber policies for data manipulation. If there's damage to digital assets, such as programs and software, as a result of hacking, the intention of the policy is to pay to recreate or reconstitute the data – but only to bring them back to the same form they were in before the attack. However the intention is not to cover any improvements to the computer network.

However if the data manipulation causes third-party liabilities, as long as it's not linked to bodily injury or property damage then it would be the intention to pay for third-party liabilities. For example if the data within a logistics platform becomes corrupt due to malicious code and as a result a third party does not receive their delivery, that third party's resulting financial loss could be covered under a Cyber policy.

We hear about a big breach every month, but in reality they're happening all the time and all around the world. The biggest issue companies face is knowing what data they have and where it is. They're always updating their assets, but not knowing the connection between them is one of the biggest issues they face in the event they are breached.

To ensure you are prepared to make a claim in the event of data manipulation you have to go back to your incident response plan. Planning and preparation are key: being prepared for it to happen, having an understanding of where your data is, what your data is and how it can be accessed, and by whom.

A good incident response plan will enable you to follow the simple steps of *identification* (how it happened), *containment* (making sure it's not ongoing), *eradication* (is it happening anywhere else?) and *recovery* (getting the data back into a working state). The crucial bit after this is looking at the lessons learnt from the experience and incorporating them into the incident response plan for next time.

QBE would like to thank Laurance Dine from Verizon Enterprise Solutions for his expertise in developing this article.

Made possible
QBE

QBE European Operations
Plantation Place 30 Fenchurch Street London EC3M 3BD
tel +44 (0)20 7105 4000 **QBEeurope.com**

8673/FEB/2018