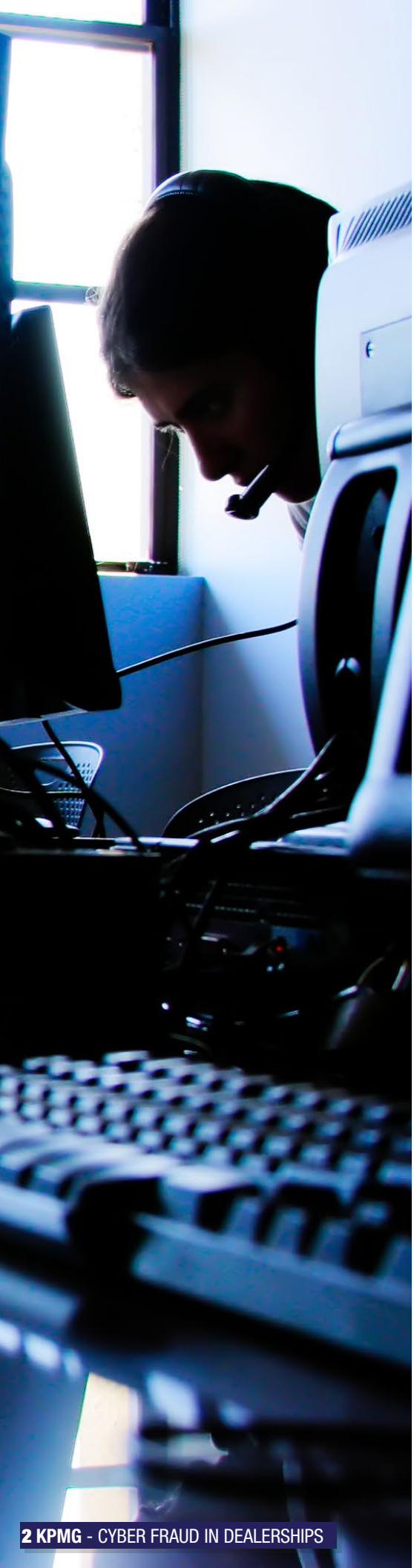
KPMG

Cyber Fraud in Dealerships

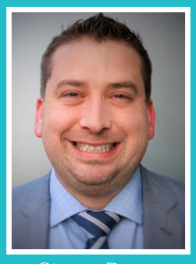
In today's world, data protection and security breaches are the new crime of opportunity... Are you at risk?

Produced by

John Mellor's GoAutoNews Premium



Contents



Steven Bragg

In today's world, data protection and security breaches are the new crime of opportunity, and you are at risk.

Steve Bragg recently joined KPMG having finished a role as the chief financial officer of a large trucking distributor and retailer.

Steve has amassed considerable knowledge of cyber fraud and how it can affect a dealership.

John Mellor's GoAutoNews Premium

Today's dealership fraud

If you think your dealership will never get hacked or suffer from a security breach, think again.

A survey conducted by Osterman Research in the USA (released in a white paper in August 2016 'Best Practices for Dealing with Phishing and Ransomware'), found:

- **63 per cent of Small to Medium Enterprises (SME) surveyed had a cyber-security incident in the last 12 months**
- **71 per cent experienced one to five ransomware infections, hacker infiltrations, malware infections etc.**

Of the 71 per cent experiencing these attacks, 18 per cent experienced six to 10 attacks, and 15 percent experienced more than 10 attacks. Although serious, losing data is one thing, but losing money is a whole other ball game, 11 per cent of companies reported CEO fraud/ business email compromise (BEC) attacks, this is basically where by pretending to be the CEO or a supplier, companies have made payments to fraudsters unwittingly.

The problem is this type of deception is on the rise. Only 27 per cent of the SMEs surveyed reported no security breaches in the last 12 months.

The survey included businesses ranging in size from 100 to 3,000 employees. The data in the report is startling, with small businesses (defined as having fewer than 500 employees, most dealerships in Australia would be included) being the most vulnerable to security attacks as they are less likely to have security experts on staff.

Figure 1

Security incidents that have occurred during the past 12 months

Problem	% of Organisations Affected
An email phishing attack was successful in infiltrating our network	34%
One or more of our endpoints had files encrypted because of a successful ransom ware attack	30%
Malware has infiltrated our network, but we are uncertain through which channel	29%
Sensitive/confidential info was accidentally or maliciously leaked through email	17%
An email spear phishing attack was successful in infecting one or more senior executives	14%
Our network was successfully infiltrated through a drive-by attack from employee Web surfing	12%
An email as part of a CEO Fraud/ Business Email Compromise (BEC) attack successfully tricked someone	11%
Sensitive/confidential info was accidentally or maliciously leaked through a cloud-based tool like	5%
Sensitive/confidential info was accidentally or maliciously leaked through a social media application	3%
Sensitive/confidential info was accidentally or maliciously leaked, but how it happened is not certain	1%

Source: Osterman Research, Inc.

So how does this affect me?

The report's findings are similar to what I have seen at my dealership clients and in my own experience while in the industry. In the last three years, the rate of these types of attacks continue to increase exponentially. The reason being, every time a hacker successfully breaches a network and profits from it, 10 more cyber criminals get into the game.

The primary target of the hacker is Service Message Blocks (SMBs) on computer networks with large amounts of data. In dealerships, there is enormous value in the customer records kept in dealership management systems (DMS) and Customer Relationship Management (CRM) applications. This, combined with weak controls and a general lack of focus on computer network security, leave dealerships open to highly destructive cyber-attacks.

Hackers will target the following:

- Information included in deal folders
- Service Repair Orders (ROs) data including your customer's name, address, phone numbers and credit card numbers
    - Deal folders contain a goldmine of high quality data about your customers that a hacker would target to perpetrate frauds on your customers and your dealership
- Login details for PCs and mobile devices that allow access to customer information such as credit reports, credit card numbers, copies of driver's licenses, vehicle insurance information and even tax file numbers (TFNs)
- Customer bank account and BSB numbers
- Dealership bank account and BSB numbers
- Access to copiers and scanners that may contain hundreds of thousands of stored digital documents
- Login details to your DMS to mine data including
    - Employee payroll information
        - TFN, Bank Account and BSB
        - Addresses and phone numbers
    - Supplier master files
        - Contact details
        - Email addresses
        - Bank Account and BSB
        - Information to extort from your dealership
    - Customer information noted above

How does the hacker get value from the data stolen?

Apart from selling your dealership's and customer's data to the highest bidder, hackers can use the information obtained in a security breach to inflict significant financial and reputational damage to your business. According to the Osterman survey, the most successful forms of security attacks included:

Phishing

34 per cent of SMEs experienced a successful phishing attack. Phishing attacks occur usually in the form of emails that appear to come from a legitimate entity or person, such as a bank or supplier. The message contains a link that takes the victim to a fraudulent website, for example, a website that looks exactly like the bank's website. The user is prompted to provide login information, which is then used by the hackers to access the dealership's real bank account.

Spear phishing

Takes the scam one step further (very scary) and targets specific individuals within an organisation. In dealerships, typically this is the controller or someone in accounts. The employee receives an email that appears to be from the dealer principal or general manager, with a request and instructions on how to wire money to an account. Typically this is accompanied with a confidential email saying a deal is being completed and that no-one else should be notified or consulted. Once the money is wired, there is no way to recover it.

The most concerning aspect of spear phishing is that the attack can take place without any actual 'hacking' required. Most of the information required to perpetrate this attack can be obtained from LinkedIn and other social media.

Virus or worm infection

29 per cent of SMEs experienced these types of attacks, which are computer programs that replicate themselves and spread through a computer network. The viruses and worms are designed to destroy data, use available memory and bring systems to a halt. Similar to the denial of use attack on the Australian Census Bureau, these attacks aren't designed to extort or embezzle. They are malicious in nature and done to shut down your systems and damage your business.

Ransomware

30 per cent of SMEs were victims of ransomware, a type of malware that infects computer networks and lies dormant for a period of time. Once activated, ransomware encrypts all files in an organization and the hacker will demand a ransom for the release (decryption) of the files. Usually they will ask for payment in bitcoin or other non-uniform methods of payment.

You may think you're protected from this by performing backups of your files. That may be the case, if your backup is not connected to your computer network and is current and up to date. Many victims of ransomware attacks have unfortunately found out too late that the backups had stopped working or that the backup was in fact connected to their computer network and encrypted as well.

The Osterman survey also found that for SMEs, overall security related costs have increased an average of 23 per cent in the last 12 months. The increase is likely correlated to the growing number of security threats. For example, as observed by the Anti-Phishing Working Group, in the first quarter of 2016 the number of phishing URLs increased by 250 per cent from the fourth quarter of 2015. Also, the US Department of Justice reported the total volume of new ransomware attacks (in excess of 4000 per day in 2016) increased by 300 per cent compared to 2015 volumes.

Phishing, and specifically highly targeted forms of phishing like spear phishing and CEO fraud/BEC, as well as ransomware, are the logical evolution of cybercrime for the foreseeable future. The theft of hundreds of millions of records from several high profile security breaches in the past few years has resulted in a glut of data/records in the marketplace. The resulting prices for stolen records in the market have plummeted. Therefore, cybercriminals are turning increasingly to more direct means of theft.

Real life examples

Example 1

Recently one of my clients was attacked using a spear phishing technique. The attack started with the accounts payable clerk receiving an email from a major supplier to update the bank details. The email came from the supplier's email address and looked legitimate. The accounts payable clerk updated the banking details in their DMS on the same day after calling the number on the email to confirm the changes. Sixty days later, the supplier chased the dealership for payment. After investigation and discussions with the supplier the dealership's administration team identified that the bank account changes were not legitimate or initiated by the supplier. Two months of payments (totaling thousands of dollars) went to an account in Australia set up by a 'mule' or intermediary which then immediately transferred the money to Russian bank accounts. The matter was referred to the Australian Federal Police and none of the funds have been recovered.

This fraud was easily perpetrated by the hackers. They identified dealership accounting staff on LinkedIn or other social media using a simple Google search. They then identify a major supplier in the dealership staff's connections on social media. The final step is cloning the email of a major supplier and providing the Australian bank account details of their local intermediary. They even changed the contact number on the email so that when the accounts payable clerk called to confirm the changes they spoke to the hacker's associate. Once the money is sent it cannot be recovered.

Real life examples

Example 2

A major fraud discovered recently was another spear phishing attack. The financial controller (FC) received a confidential email from the DP/owner detailing an urgent deal that was taking place. The hacker found the FC's personal email on LinkedIn and easily determined who the DP/owner was based on the FC's connections. The hacker cloned the DP's email address. The first email was innocent and nothing out of the normal asking the FC if he was available later in the day to help him with a project. The email expressly stated that the DP would be tied up in confidential meetings and would not have access to his phone. This email laid the path for the fraud.

Once the FC replied in the affirmative, the next email confirmed that a confidential deal was taking place and that a deposit of $500,000 would be required ASAP. Once the FC confirmed that it could be done the hacker sent the Australian bank BSB and account details. Of course, the account belonged to an intermediary of the hacker and as soon as the money arrived in the account it was transferred overseas. The AFP were contacted once the fraud was uncovered, however the funds were never recovered.

Similar spear phishing attacks have been taking place at OEMs globally and in Australia for years now as hackers target the largest companies first hoping for the biggest returns for their efforts. The hackers clone the email addresses of high level executives. They then follow a very similar approach to the above and bait the finance team into sending large sums of money to fraudulent bank accounts.

Real life examples

Example 3

Other recent attacks in the Australian automotive industry include typical virus infections and ransomware attacks. Australian OEMs and dealerships have noted a spike in ransomware attacks where employees receive files or links in emails that once opened or clicked encrypt all files on the host computer and any computer connected to it by the company's network.

The hacker's demands ranged from 5000 Bitcoins to hundreds of thousands or millions of dollars. The only way to recover the data is to pay the ransom. All the dealers and OEMs in these instances didn't pay or were not willing to disclose if they did pay the ransom. In some instances we noted the hackers continued sustained attacks on the dealership until they did pay, if the ransom wasn't paid in the first instance.

There are countless examples in Australia and in the US where these ransomware attacks have destroyed small businesses to the point of closure as they were unable to recover vital data and unable to pay the ransom.

Who is perpetrating these attacks?

Criminal gangs locally and overseas have employed hackers to carry out these attacks. Combining the gang's criminal networks (some multi-national) with the hacker's abilities to infiltrate computer networks, obtain valuable data and extort financial gain from the organisations they target. Fraud and embezzlement is no longer just limited to your dealership's employees. Your dealership can and is highly likely to be targeted. Early detection and prevention of these attacks is key in protecting your business.

How can dealerships prevent security breaches?

The consequences of a security breach can be especially costly for a dealership, not only financially, but also in the loss in consumer trust and confidence. The good news is it's actually not that difficult to prevent these types of intrusions. Dealerships can minimise the threat posed by phishing, viruses and ransomware by doing the following:

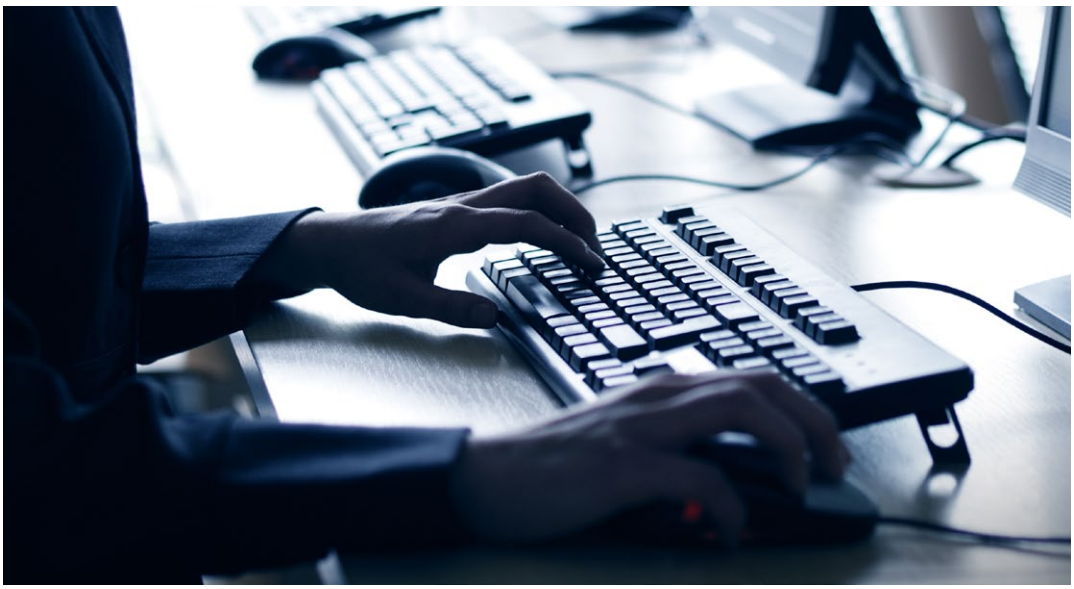
- Don't click on links in emails or download documents sent by an unknown party (email 101)
- If you receive an email from your bank, don't use the link to go to the bank's website. Instead open a new window to navigate to your bank's website. If you have any concerns about the content of the message you received, call your bank on the phone number you normally use or call their central number to ensure your speaking with the bank and not the hackers
- Require verbal authorisation for all email requests to wire or transfer money. Revisit your banking controls in general. Ensure the person who loads the EFT payments are not able to authorise/approve them. A strong control (if you have the ability) is to require a minimum of two authorisations for any wire transfer/EFT
- Employee training and awareness of the threat to your business from cyber-attacks is key as your employees are the last line of defense during an attack
- Keep every computer's operating system and other software applications up to date, installing patches and updates regularly
- Use firewall and antivirus software, the software needs to be updated regularly to ensure it prevents the latest forms of infiltration into your servers
- Invest in a good Information Security and Privacy Liability insurance policy. Traditionally, property insurance policies protect your dealership from physical losses related to damage of property, but they may not pay for costs related to the loss of data or financial embezzlement.

What do I do if my dealership has been hacked or I suspect there has been a breach in my IT systems?

You've been hacked. The hackers have infiltrated your server and have access or accessed confidential customer and dealership data. Your first instinct is to kick them out and close the weakness in your network that let them in. Its human nature, someone is in your house and your first instinct is to get them out.

However, your best course of action is to seek professional assistance to ensure you fully understand where they infiltrated your network (there may be several back doors or weaknesses in your network) and what exactly they have accessed. Even better, if you can catch them in the act the authorities have a better chance to find the hacker(s) and to prosecute them.

The best course of action is to immediately get the proper professional assistance and involve the authorities in the first instance. You can then assess the damage and repair your network after a full understanding of the attack is determined.



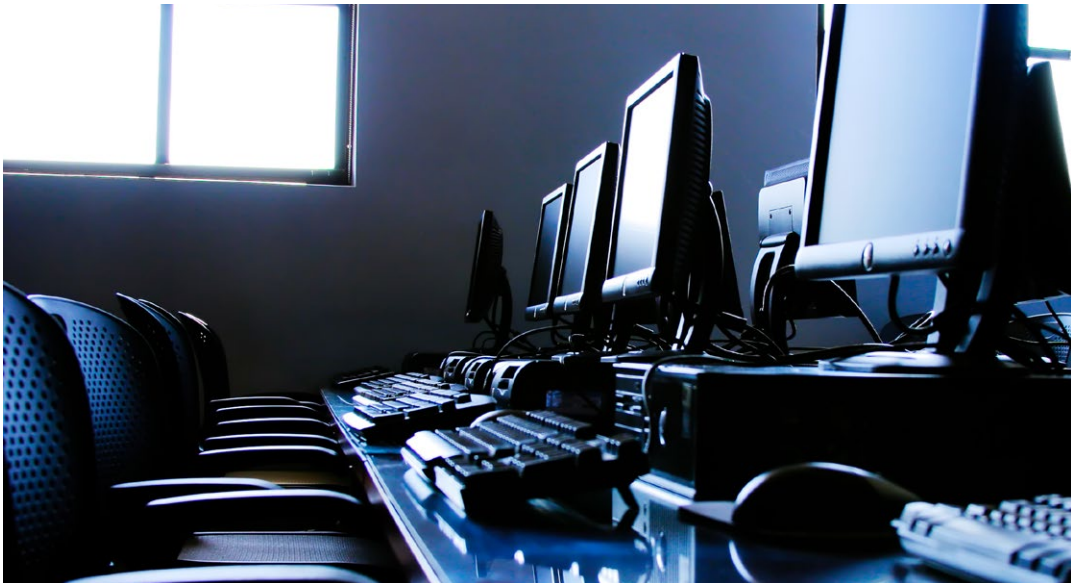
What to do if I have been a victim of embezzlement from a hacker or employee?

Once the embezzlement has been confirmed, document everything and contact the appropriate public authorities (police, AFP etc). Understand the how, when, and the total impact of the fraud. In conjunction with your internal investigations, you may need professional assistance if you don't have the capabilities in-house.

Most importantly, and despite the difficulty, you must prosecute the fraud fully to the extent of the law. In my own personal experience, this takes a significant amount of time and you may not get significant assistance from the authorities.

They either don't understand or are not interested in prosecuting these types of crimes. However, the most important prevention mechanism in your fraud prevention framework is the environment and tone set from the top. If you don't prosecute a fraud identified, the message this sends to your dealership employees is contrary to prevention.

A combination of technology solutions and employee awareness and training are required to keep hackers at bay. Every dealership should have a security policy and make sure the recommendations are followed and kept up to date.



Conclusion

Fortunately, the days where fraud was about following the money are pretty much over. Back when:

- **the used car manager and the wholesaler conspiring to overvalue trades and splitting the difference;**
- **duplicate bank accounts in payroll; and,**
- **the sales person keeping the vehicle deposits and changing the deal paperwork.**

Unfortunately, with technology pushing everything online and most communication today done electronically rather than over the phone, the opportunities have increased, the criminal is faceless (and often across the globe) and it's now a percentage game due to the anonymity.