Vermont's Technology Times

"INSIDER TIPS TO MAKE YOUR BUSINESS RUN MORE PROFITABLY, FASTER AND SECURE"

January 2022

Phenomenal IT Support For Business
www.vermont.co.uk

Inside This

The Average Time to Identify a UK Data Breach is 181 days

A key factor in determining the damage caused by a data breach is how long it takes a company to remediate an incident. In the UK, organizations took an average of 181 days to identify the fact that a breach had occurred, and a further 75 days to contain the incident. With a total of 256 days for identification and containment, the UK was fifth fastest to respond, behind Germany, Canada, South Africa, and the US.

A Tale of Two Ransoms

You might of noticed in the last few years that Insurance Brokers have been talking about Cyber Crime Cover (and hopefully your IT support company have too). This is in direct relation to the dramatic increase in Ransomware, stolen credentials and CEO Fraud experienced by every type, and size, of business and organisation. In the UK, according to the Police, 49% of all reported crime is Cyber related, and the National Fraud Intelligence Bureau (NFIB) tracked losses resulting in £1.9 billion in 2020.

Now you might think it won't happen to you, or the impact won't be too bad if you did get hit. Sorry to burst your bubble, but it's a case of when and not if. And the impact could be bad.

You've heard that all before though, right? IT companies scare mongering, so why is now any different? Why should i be paying attention? You can no longer shrug this thing off as the game has changed and you need to know what to do.

They are even smarter than you think

I was on a conference call with 2 of my peers, who were presenting 2 case studies about breaches/ransom's they both had worked on in the last year. Neither of them could share the names of the client's because of legal restriction, but what was really interesting was that one had cyber Insurance and the other didn't. And I think you should know the difference between the two when dealing with a ransom.

How did they get in?

First thing everyone wants to know is how did they get in? In Company A's case (uninsured) it was through the Microsoft Exchange vulnerability that came to light last January 2021. IN B's situation (insured) it was through stolen credentials. In both cases there were oversights by the in-house IT teams, which lead to the ransomware being deployed, and the Bad actors (Hackers etc) had got into the system (Jan 2021 for A) 6 months before the ransom took place (July 2021 for A).

Continued on pg.2

Continued from pg.1

Why the delay? The forensic specialist who worked on 'B' educated my colleagues on the processes, tools and operating procedures that these gangs use. Essentially there are gangs (lets call them Inside Sales) that find the initial compromise (i.e the point of entry), do reconnaissance on the victim (find out how much money they have), install backdoor ways of entry (usually between 6-8 ways of entry), then sell the opportunity on the Dark Web to 'Sales Team' gangs (in this case the 'Conti Group'). This team will then go on to deploy the ransomware and then extort money from the victim.

The delay is because the Inside Sales teams are finding lots of opportunities (i.e. Compromised victims), far more than the Sales Team can work on, and so there is a backlog. The deployment of the code doesn't take long, nor the extortion negotiation, but having that extra time to do reconnaissance gives them more data to leverage.

What happened to all the Tech protection? In the Insured case, one of the markets leading Next Gen Anti-Viruses identified the exploit after 95% of the environment had been encrypted. In Company A's situation, the AV had picked up an issue but it was never investigated. But then how did the ransomware file get through the firewall? That's because the Bad Actors had access to the system and could do what they want at that stage.

Why wasn't the Exchange server patched? In Company A they had an in-house person who had attempted to install the patch but it failed, and after 4 or 5 attempts they gave up. So it went un-patched. And that's the cause - bad hygiene leads to problems.

What happened straight after the systems were encrypted? In company B's case their IT provider got straight on it - called the Insurance company and then worked 40 straight hours restoring and rebuilding systems. But they weren't alone - the Insurance company deployed a lawyer, ransom negotiator, forensic analyst, and remediation experts.

In fact, the Insurance company took charge of the situation and managed the whole process. In Company A's case, they wasted 48 hours choosing a Security Remediation company! They also had to find a ransom negotiator, pay another third party to pay the ransom, re-train staff to rebuild desktops, and work with a Lawyer.

What were the Losses? The uninsured company ended up paying $175k in extortion fee's (and a further $15k to a third party to make the payment), plus they made their employees take holiday or unpaid leave to limit their losses. In total, $300k, plus 4 days of downtime and a further 3 weeks till the system was back to fully operational. Company 'B' only lost 4 days in downtime. The insurance company covered all of the remediation fee's and there was no ransom/extortion fee paid.

What can you do? The best strategy to take when it comes to cyber crime is to take a proactive approach in protecting yourself, and then have the necessary insurance and processes in place when you do get breached:

- **Hygiene:** To make it hard for hackers to do damage you want to make sure you have the right balance of hygiene and tools.
- **Tools:** It's no good having a bunch of tools if there is no checking that they are set up right, up to date and operating as they should be.
- **Training:** Your staff are the biggest threat to your system integrity. Train your staff regularly.
- Insurance: Get insurance cover for Cyber.

Oh, and with the extortion thing, be prepared for the hackers to call your staff and tell them lies, give bomb threats, and all other sorts of nefarious stuff.

What you going to do now? Call your broker and get talking to them about including Cyber cover if you haven't got it.

If you have it, talk to your IT team to give them the details on who to call, so they can get the process on what to do and who to call documented.

Shiny New Gadget Of The Month:

Biolite Firepit+

Campfires are a camping tradition that brings people together to talk, relax or even cook. But the main problem with campfires is the smoke. It gets in your face, hair and clothes – and can ruin an otherwise relaxing evening.

For this reason, BioLite created the FirePit+. This is the upgraded model of their classic FirePit and creates hyper-efficient flames by using patented airflow technology that can erase smoke. FirePit+ is Bluetooth-operated and comes with a mesh screen that allows for visibility from any angle. It's not just a firepit either. You can put charcoal underneath the fuel rack to turn the FirePit+ into a grill.

Although, the reviews on Amazon seem to say that there is still plenty

Don't Give Up On You

As you venture through your business and personal life, you'll have people tell you "no" or that your ideas aren't good enough. But remember: you know your goals, dreams and aspirations better than anyone else, so why would you let their opinions have an impact on your vision? I certainly wouldn't be where I am today if I had listened to all of the naysayers and critics. If you have a dream, don't let anything hold you back from accomplishing it.

After I wrote my first two books, *The Toilet Paper Entrepreneur* and *The Pumpkin Plan*, I approached my publisher and said I had written another book: *Profit First*. They looked it over and said, "Nobody needs another accounting book." I was a little stunned, but I wouldn't let that stop me.

I knew that I had a really strong book, and my mentor at the time told me to "make them regret it," so I doubled down and decided to publish *Profit First* myself. It ended up being a roaring success. I sold so many copies that my publisher reached out to me about buying the book after they had rejected it the first time!

We made a revised, extended edition for Penguin Books, and it is definitely my most popular book to date. If I had listened to my publisher the first time around, I never would have made *Profit First* or any of the other small-business books I have written since then. I get calls and e-mails all the time from small-business owners who have improved their businesses through things they learned in *Profit First*. All of the money these businesses saved and the lessons they learned from *Profit First* never would have happened if I have given up on my goal.

If you come up with a product, service or idea that you think can help people in any regard, try to push forward through any negativity or criticism. Critics don't always see the big picture and may use preconceived

Mike Michalowicz is a very successful author, entrepreneur and lecturer. He has written several successful books, including his latest, Get Different. *He is currently the host of the "Business Rescue" segment on MSNBC's* Your Business, *and he previously worked as a small-business columnist for* The Wall Street Journal.

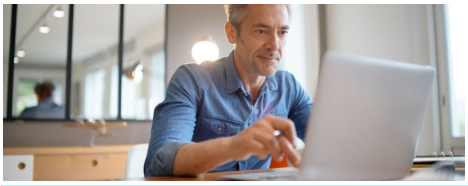
New Team Member—Matt

Stott joined the Team in November 2021, after working at a number of IT companies, around the Solent area since leaving college in 2014 (where he studied IT and Software).

He currently is our number one ticket closer on the helpdesk, just in front of

Angus, and speaks to at least 10-15 users everyday. Being on board for only 3 months he has shown how capable an Engineer he is, getting up to speed quicker than we all imagined.

At the time of writing Matt is going on honeymoon to the Cape Verde Islands. When he is not working for us he goes to the gym 3 times a week, is a massive Arsenal fan (that's two of us at Vermont) and is an avid foodie.



Favourite Music artistes are: Childish Gambino, David Bowie, Moby

The other thing of note is that he is extremely knowledgeable on tech stuff, tropical fish, rabbits and his favourite foods are: Pumpkin Katsu Curry, Pad Thai, Schupfnudeln!

Valuable Insight from Our Insurers:

I asked Trevor Cornbill at our Insurers, Morrison Solutions, for his view on the state of the Cyber market currently (leading on from the front page) and this is what he said:

'The manufacturing, wholesale and distribution sectors continue to be particularly challenging areas from a

loss perspective. These sectors appear to be being targeted by cybercriminals and as a result, manufacturers, wholesalers and distributors have not only seen an increase in the frequency of ransomware attacks over recent years, but an increase in the severity of ransomware attacks too. You may have noticed recently that other Insurers have pulled out of manufacturing completely.

Unfortunately this trend has meant that we have now had to take corrective action in the rating to avoid having to pull out ourselves. This is why the increase at renewal is so substantial this year. I appreciate that this is a huge increase compared to last year but unfortunately the only alternative would have been to non-renew. To be able to continue writing business in these sectors sustainably this is the rating that would have to be achieved.

As I imagine you aware there have been several high profile, such as BlackBaud, SolarWinds and Kaseya in the last 12 months and therefore given the current economic climate it no surprise that premiums seem to be increasing. The other big change seems to be towards whether or not you have MFA, if you don't then insurers won't quote, which is a big change from previous years.' www.morrisoninsurance.co.uk

Cyber Stats: 13% of UK organisations ended up paying the ransom

In the attacks that were successful in 2021, around 13 percent of UK companies went ahead and paid the ransom demanded by cyber criminals. This was well below the global average of 26 percent and far lower than the top payers. In India, 66 percent of organizations paid while in Sweden, the figure was 50 percent, and in the Philippines, 32 percent.

Who Else Wants To Win A £25 Gift Card?

You can be the Grand Prize Winner of this month's Trivia Challenge Quiz! Just be the first person to correctly answer this month's trivia question and receive a £25 Amazon gift card. Ready? Call us right now with your answer!

Where did Google founders go immediately after getting their first investment check?

a) Burger King
b) Wells Fargo
c) BMW Dealership
d) Disneyland

Call us right now with your answer! 02380 983405