Data Breaches and Cyber Attacks: Tis’ the season to be concerned

MOORE ClearComm

Today's Webinar

- Cyber Crime Seasonality
- The Christmas Trend
- Festive Closedown Tips
- 2024: What to Expect Next Year
- Opportunity for Questions

Today`s Panel:

Maritz Cloete and Paras Shah

"It`s the most vulnerable time, of the year…"

Andy Williams

MOORE ClearComm

CYBER CRIME SEASONALITY

It`s Christmas time…

- 30% increase in average monthly number of ransomware attacks over the holiday period (*Darktrace*)
- 70% increase in attempted ransomware attacks in November and December, compared to January and February (*Darktrace*)
- Surge in online shopping, social media usage, and digital communication
- Cyber attackers use increased internet traffic to target unsuspecting users who may be less vigilant
- IT and Security Operations teams are often short-staffed over Christmas and New Year
- Attacks may take place while a business or organisation is closed – remaining undiscovered for days
- 70% of IT respondents surveyed, admitted to being intoxicated while defending their company against ransomware during the holiday season (*Cybereason*)

Why is Cyber Crime “worse” for businesses at Christmas?

- More likely to be attacked by cyber criminals than at any other time of the year
- Risks are higher due to lapses in workplace vigilance and unattended systems
- Heightened team mood and positivity, leading to lowered diligence and risk concern
- Distracted employees due to pressures of the season
- Organisations either winding **down** for Christmas closure, or
- Winding **up** for their busiest time of the year
- Mental health and anxiety: stress, finances, loneliness – all impact on employee cyber diligence

Accidental Data Breaches

- In the final week before annual leave or seasonal holidays
- Mid to late afternoon (due to fatigue, approaching end of the day or rushing to do the school run)
- During periods of high stress, pressure and anxiety
- When rushing to clear desks or workloads before a weekend
- Friday`s between 3pm to 5pm:
    - Peak timing for accidental data breaches
    - Most likely time that phishing emails will be “clicked”
    - When we are most exposed to Business Email Compromise (BEC)

Case Studies and Examples

Arnold Clark (Car Dealership) Breached: 23rd December 2023

- Suspicious activity detected
- Network was closed off from the internet, availability issues and disruption

Royal Mail Ransomware Attack January 2023

- The threat of publishing stolen information after recent postal strikes
- Temporarily Unable to send letters or parcels abroad
- Millions of pounds of losses

Case Studies and Examples

Guardian Ransomware Attack December 2022

- Locked users out of London offices
- No access to key systems such as print production and payroll

Vatican Website Taken Down December 2022

- Occurred the day after Moscow criticized Pope Francis's condemnation of Russia's invasion of Ukraine
- Cyber attacks are seen as a hallmark of Russian warfare, escalating following the country's invasion of Ukraine

THE CHRISTMAS TREND

Common Christmas Scams on the Public

- UK spends more money at / on Christmas than any other nation in Europe
- £30.91bn is forecast to be spent online by UK shoppers this Christmas
- 23 million (43%) will use credit cards to cover their Christmas spending this year
- £14 billion will be spent on credit cards
- 61% of GenZ will use credit cards to cover their Christmas costs

Exposing us to:

- Charity fraud
- Cost of living scams
- Travel / holiday fraud
- Banking and digital payment scams
- Fake delivery updates (SMS, Email)
- Fake (shopping) websites

December Threats

- WhatsApp “colleague request” scams
- Business email compromise (BEC)
- Phishing emails
- Ransomware
- Malware
- Distributed Denial of Service (DDoS)
- Attacks on eCommerce websites

“Cybercriminals know companies are less responsive during the holiday season and therefore tend to strike at this time.”

German Federal Office for Information Security

MOORE ClearComm

Christmas Period Attacks on Business

- Christmas period is a deliberate target
- Attackers plan for weeks / months in advance
- They know they can often work undetected
- Organisations reduced to minimal IT / technical teams
- Most have inadequate IT response contingency
- Christmas attacks are more impactful on business
- More likely to be reported in the media (fame)
- Peak shopping period: ransom is more likely to paid (or paid faster)

FESTIVE CLOSE-DOWN TIPS

Tips for a More Secure Christmas

- Use different passwords for your online accounts and enforce MFA where available
- Ensure operating systems and all applications are up to date, patching your systems as early as possible after updates are released
- Ensure firewall controls have a valid business use case and have been audited.
- Consider a pre-holiday audit or vulnerability assessment of all your internet-facing assets
- Promote staff awareness and educate users on what to look out for considering cyber threats

Tips for a More Secure Christmas

- Establish a secure and supportive environment where staff members feel comfortable and encouraged to report any suspicious activities or concerns
- Ensure critical data is backed up and the recovery process is tested regularly
- Have an up-to-date and tested incident response plan in place which also considers staff shortages during holiday periods
- Keep your social media/digital footprint small and focused
- Cybercriminals don`t need to know all your staff will be away or that you`ll be operating on a limited team during the holidays

Your Plan for 2024

Make a commitment to continuously improve your company's cyber security posture in the coming year:

1) Take the time to understand where your organisation may be vulnerable to cyber attacks

2) Build these areas into your improvement strategy for the new year:

- Systems: old systems, lack of software updates, poor security configuration, lack of monitoring
- People: lack of cyber security (and data privacy) awareness, weak policies and procedures
- Business processes: poor business security practices, insecure data sharing internally or with third parties and suppliers

3) Consider investing in Phishing simulation and training

Your Plan for 2024

4) Commit to Cyber Essentials - get the basic cyber hygiene factors right

5) Test your defences:

- Commission vulnerability scans and / or penetration tests and
- Test your response capability (i.e. simulate a cyber attack)

6) Don't forget about your suppliers:

- Map out who you share systems and data with
- Ensure their security posture matches your risk appetite

2024:
WHAT TO EXPECT NEXT YEAR

2024: What to expect during and from next year

- Geopolitical Uncertainty / Conflict / Nation State-backed attacks
- Artificial Intelligence: increasingly deployed by Cyber Criminals
- Smarter and more sophisticated phishing tactics
- Cyber security presence emerging on the boards of companies
- Internet of Things: weaponised against businesses
- Regulation: Product Security & Telecommunication Act - comes into effect on 29 April 2024
- More companies asking for their suppliers to hold Cyber Essentials or Cyber Essentials Plus

QUESTIONS

maritz.cloete@mooreclear.com

paras.shah@mooreclear.com

richard.jackson@mooreclear.com

Our next webinar

“Human Firewall: Your People and their Role”

Date: Thursday 18th January 2024
Time: 10.00am-11.00am

Moore ClearComm Speakers:

- Rich Jackson, Strategic Business Manager (Moore ClearComm)
- Bob Harper, Founder (Agendali)
- Paras Shah, Cyber Security Consultant (Moore ClearComm)

Location: Zoom

MOORE ClearComm

Moore ClearComm
9 Appold Street
London
EC2A 2AP
t: +44 (0)20 45821983

www.mooreclear.com

MOORE ClearComm