Newport Consulting

Powerful Insights & Expertise

Incident Response Management after a Breach is Detected

Newport Consulting

Powerful Insights & Expertise

Company Contact Information

| www.thenewportconsulting.com

| contactus@thenewportconsulting.com

| linkedin.com/company/newport-consulting-llc

Newport Consulting
Powerful Insights & Expertise

Carl Grifka

carl.grifka@thenewportconsulting.com

Carl Grifka, Principal, Newport Consulting LLC & Chief Financial Officer, Cinionic

- Carl is a dynamic Finance and IT leader specializing in finance, IT security/risk, project management, lean process design, and risk advisory solutions.
- Carl is leading Newport Consulting LLC's IT consulting division and new international Flex Specialist Center. Carl is also the CFO/Compliance Officer leading Cinionic's finance department and global initiatives to finance new OPEX service models in the cinema industry.
- Prior to joining Newport Consulting LLC and Cinionic, Carl was a worked in consulting at RSM LLP specializing in IT and Finance advisory, in internal audit at General Motors, and as a revenue agent for the Internal Revenue Service.

Education

- Certificate, Executive Leadership, Cornell University
- Master of Science, Finance, University of Michigan
- Bachelor of Arts, Accounting, Michigan State University

Certifications

- Certified Information Security Manager (CISM), ISACA
- Certified Information Systems Auditor (CISA), ISACA
- Project Management Professional (PMP), PMI
- Certified Data Privacy Solutions Engineer (CDPSE), ISACA
- Lean Six Sigma / Design for Six Sigma Green Belt, Aveta Business Institute

Newport Consulting
Powerful Insights & Expertise

Andy Portillo

andy.portillo@thenewportconsulting.com

Andy Portillo, Cybersecurity SME, Newport Consulting LLC & Vulnerability Assessment Manager/Part-Time Lecturer, University of Southern California

- Andy brings with him over seven years of experience in a wide range of information technology (IT) and cybersecurity disciplines, gaining extensive information security experience through roles including IT auditor (RSM), information security analyst, penetration tester and lecturer at a large R1 university (USC).
- Andy processes deep technical and experience in the financial, payment card and academia industries.
- Andy's focus will be to aid in the end-to-end vulnerability remediation efforts across an organization and to provide an excellent customer experience throughout the entire process.

Education

- Master of Science, Info Assurance and Cybersecurity, Capella University
- Bachelor of Science, Info System and Cybersecurity, ITT-Technical Institute
- Associate of Science, Computer Networking Systems, ITT-Technical Institute

Certifications

- Certified Information System Security Professional (CISSP), ISC^2
- Offensive Security Certified Professional (OSCP), Offensive Security
- GIAC Enterprise Vulnerability Assessor (GEVA), SANS
- GIAC Web Application Penetration Tester (GWAPT), SANS
- Certified Information Systems Auditor (CISA), ISACA
- Certified Data Privacy Solutions Engineer (CDPSE), ISACA

Newport Consulting
Powerful Insights & Expertise

Timothy Towne

tim@ine-solutions.com

Timothy Towne, Cybersecurity SME, INE Solutions

- Tim is a certified cybersecurity engineer with over 25 year's experience in the U.S. Intelligence and DOD space. Tim currently works with small and medium size commercial companies to help them understand and implement cybersecurity governance and technologies.
- Tim believes providing timely analysis and information to decision-makers is key to developing an organization's overarching tactics, techniques, and procedures (TTP) to deal with today's evolving threats and vulnerabilities.
- Tim has worked with several C-level equivalent government personnel to deliver timely and effective decision-making processes and procedures.

Education

- Master of Business Administration in Management Information Systems, California State University
- Bachelor's Degree in Percussion Performance, California State University

Certifications

- Certified Information System Security Professional (CISSP), ISC^2
- Information Systems Security Engineering Professional (ISSEP), ISC^2
- Certified Cloud Security Professional (CCSP), ISC^2
- Security+CE certification
- Cybersecurity Maturity Model Certification (CMMC) Registered Practitioner (RP)

Newport Consulting
Powerful Insights & Expertise

About Newport Consulting LLC

Finance | Tax | IT Risk & Cybersecurity

Mission

- Deliver market leading accounting, tax, and IT expertise with our industry professionals
- Provide unmatched flexibility with subscription offerings to provide our expertise when you need it
- Offer cost effective solutions leveraging our international resources

Values

- We act with a sense of urgency
- We do the right thing
- We pay attention to detail

Qualifications

- Our experts include those with Big 4 accounting firm and large Fortune 500 company industry experience
- Professional designations include market leading certifications for public accounting, IT risk / cybersecurity, project management, and lean process
- Advanced degrees within accounting, IT, and finance

Newport Consulting
Powerful Insights & Expertise

Scope of Services

ACCOUNTING & FINANCE

- Accounts payable and receivable
- Bookkeeping services
- Financial reporting & Analysis
- Accounting as a Service

TAX

- Individual tax returns
- Corporate, partnership and fiduciary returns
- Sales tax returns

FINANCE & IT RISK ADVISORY

- Internal audits & workpapers
- SOX / FDICIA compliance
- ITGC Controls Testing
- SOC 1 & SOC 2 Readiness
- Policies & procedure review
- Test of design / Test of controls

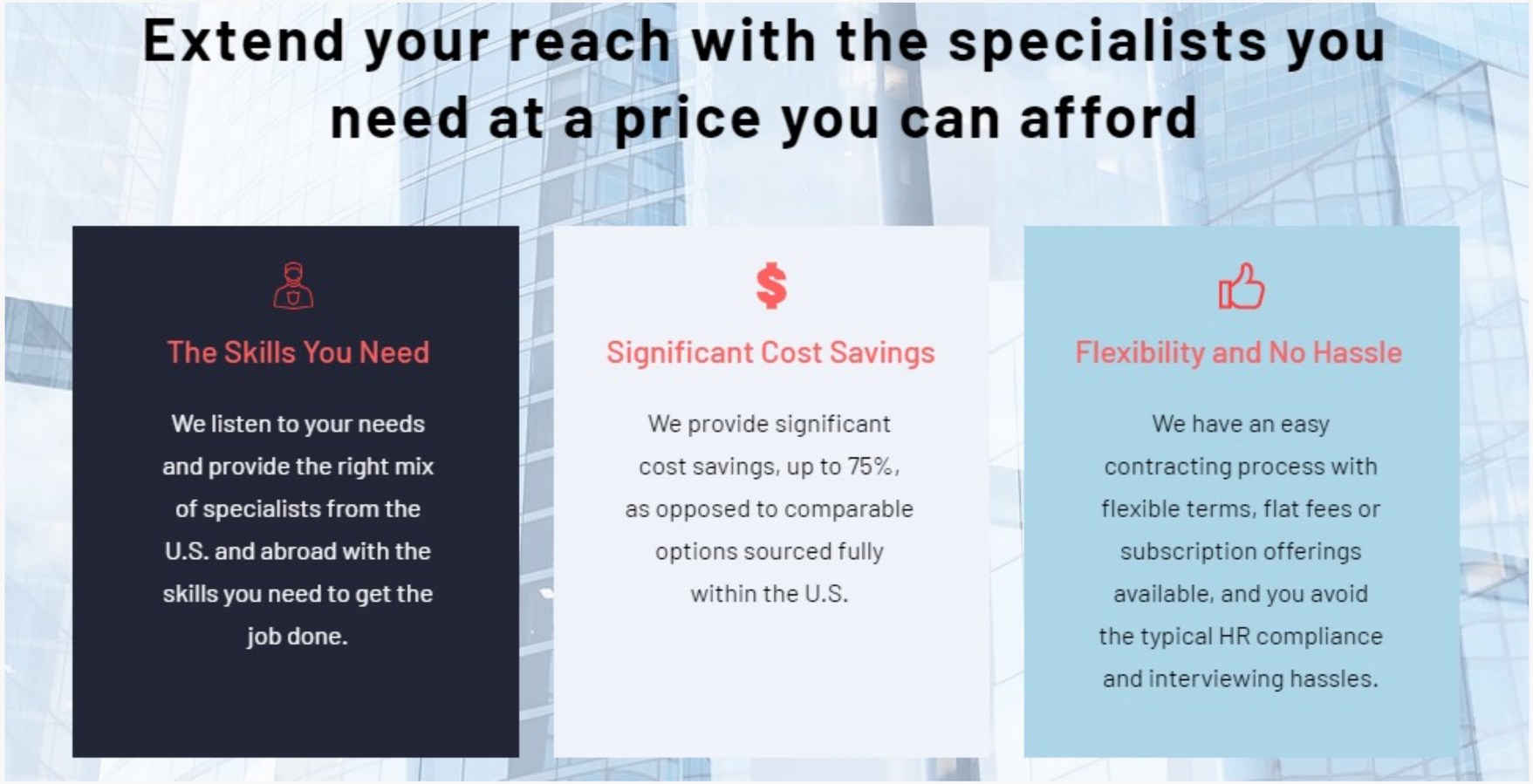
IT & CYBERSECURITY

- Information security management system implementation
- SIEM selection, implementation, and ongoing monitoring
- Cybersecurity policy, procedure, and controls advisory
- Cybersecurity penetration testing
- Incident management, testing, and response advisory

Newport Consulting
Powerful Insights & Expertise

International Resources

Using our Flex Specialist Center, we can provide international cost-effective flexible Finance/Accounting, IT Risk/Advisory, and Cybersecurity resources.



Newport Consulting
Powerful Insights & Expertise

Agenda

Overview of The Breach

1. An overview of a real-life incident involving a system breach of a company's Office 365 cloud infrastructure by a bad actor outside of the US via a spear phishing attack, resulting in a misappropriation of assets.

Incident Reponse Plan & Exposure Mitigation

2. Procedures used at time zero of the breach detection and afterwards between multiple business units to prevent additional exposure

Impact & Root Cause Assessment

3. Determine the total impact to the company. Investigate the root cause and nature of the breach.

Control Review & Implementation

4. Implement controls internally to prevent recurrence, and additional business required from the company's vendors. Brief outlook of the prevalence of these attacks and vulnerabilities.

Newport Consulting

Powerful Insights & Expertise

Overview of the Office 365 Breach

Newport Consulting
Powerful Insights & Expertise

Office 365 – Spear Phishing Incident

A targeted attack on a company's Finance department users

- Using publicly available data, such as LinkedIn, a bad actor targeted the Finance department users of a $200M+ revenue company
- Using a campaign of spear phishing emails over a long period of time, a finance user in Accounts Receivable is believed to have entered their password in response to an email solicitation
- The finance user was unaware of the mistake and continued to go about their business
- The bad actor mines the information entered to attempt to access the Office 365 environment

**We will review additional scenarios at the end of the presentation*

Newport Consulting
Powerful Insights & Expertise

The Breach Occurs

A bad actor located abroad uses the stolen credentials to access the Finance AR employees e-mail and Office 365/Sharepoint environment

- The organization's internal Sharepoint and OneDrive files, as well as key finance department shared files, were accessed by the bad actor
  - The bad actor did not deem the information accessible on Sharepoint was sensitive and no impact occurred from this information being reviewed
- The bad actor monitored the user's email box and quickly realized that it was their key to a monetary advantage
- The bad actor began to monitor the mailbox traffic, logging in at various hours in and outside of normal business hours, to determine where they could exploit the situation to steal from the organization

Newport Consulting
Powerful Insights & Expertise

Exploiting their Access

Outlook mailbox rules were rewritten and conversations were hijacked

- The bad actor monitored email traffic found a client that owed the company ~$250k in aged invoices
- The bad actor waited for the moment that the client was preparing to pay the invoice, which is when they sprung into action
- Mailbox rules were rewritten to move emails received from this client to a new folder, which could then be deleted
- The bad actor began writing emails to the client
- The bad actor provided a falsified payment instructions document, which stated that the company's auditor is directing all payments to go into a new bank account in Asia Pacific in a different company's name

Newport Consulting
Powerful Insights & Expertise

Misappropriation of Assets

The client took the document as authentic as it came from the correct email address

- The client used the falsified payment instruction and made a ~$250k payment to the bad actor's account
- The client stopped communicating with the bad actor and the client as the payment was assumed to be made at the correct amount in good faith
- The bad actor deleted all e-mails on the matter and deleted their custom email rules
- The bad actor ceased logging into the account
- Two weeks pass before the breach and misappropriation are detected…

Newport Consulting

Powerful Insights & Expertise

Incident Response Plan & Exposure Mitigation

Newport Consulting
Powerful Insights & Expertise

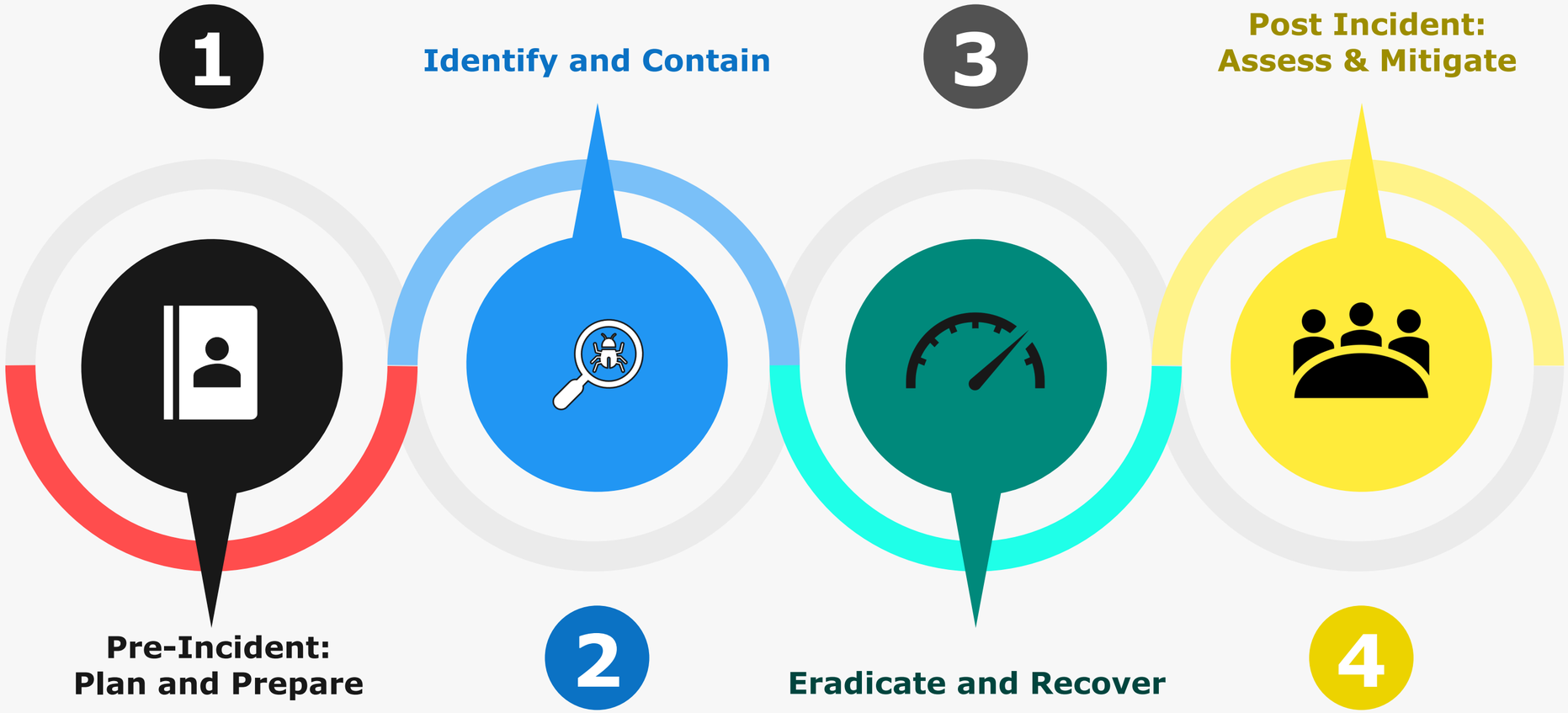
Breach Detection – Time 0

The breach is finally detected by operational Finance

- During the normal course of business, the AR analyst sends the account statement, containing all overdue invoices, to the client. The customer statement was sent approximately two weeks after the misappropriation of assets occurred
- The client reviewed the statement and escalated to their leadership and to the company's leadership, indicating the invoice was already paid
- The company received evidence of the email traffic from the client, as well as proof that the client paid the invoice as instructed via the exploited email account
- The AR analyst escalated the situation to the Controller and CFO, who initiated the incident response plan

Newport Consulting
Powerful Insights & Expertise

Incident Response Plan

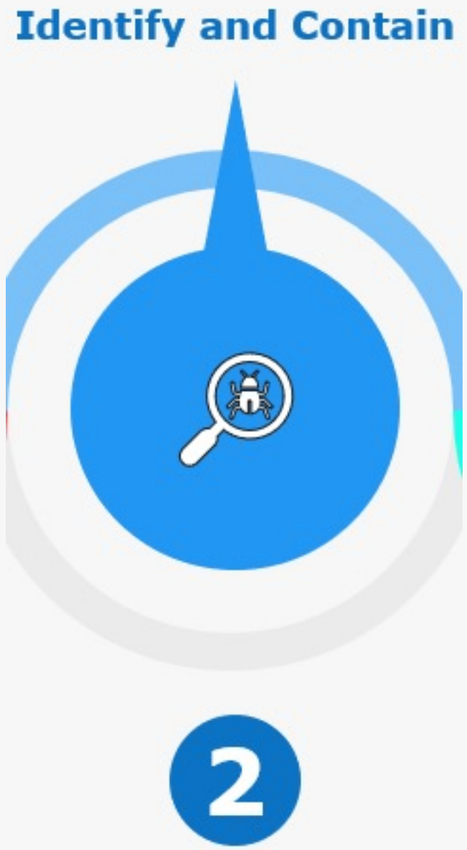


Newport Consulting
Powerful Insights & Expertise

Identify and Contain

The Incident Response Plan is Activated by the CFO and Containment Begins

- The CFO contacted the CIO to perform triage. Based on the information available, the AR analyst's account was disabled by IT to prevent additional exposure – the immediate threat was contained
- The IT organization began a forensic exam of all login, file access, and email activity in the Office 365 environment on this account. Documentation of all steps performed after time zero of the breach were forensically maintained by the minute with each action owner identified
- All members of the company were ordered to change their passwords within 24 hours. Finance team member accounts were scrubbed to validate they have not been compromised
- Finance reviewed its files on the Sharepoint and OneDrive environment to determine if any risk to the company exists from shared files
- Email settings and messages were reviewed in detail to determine possible other client exposures
- Police report was filed by both companies related to the misappropriation of assets

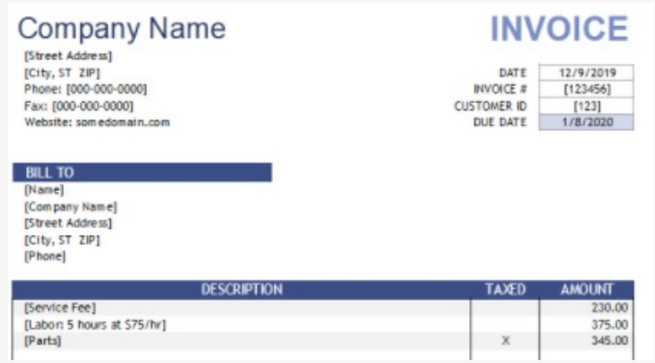


Newport Consulting
Powerful Insights & Expertise

External Complexity

Dialogue continues with the impacted client

- Management contacted the client, which has in the interim performed their own forensic analysis
- The client confirmed that the e-mails came from the company's environment as they were digitally signed from its Office 365 Microsoft domain
- The client contacted their insurance policy to determine if this loss is within the scope of the policy
- The client confirmed that they did not call-back the change in payment method, which was a failure of their own preventative management control
- The client refused to pay the $250k invoice again as they acted upon an order from the account of the AR analyst for the initial payment, which was validated to come from our environment



Company Name

[Street Address]
[City, ST ZIP]
Phone: [000-000-0000]
Fax: [000-000-0000]
Website: somedomain.com

INVOICE

DATE	12/9/2019
INVOICE #	[123456]
CUSTOMER ID	[123]
DUE DATE	1/8/2020

BILL TO
[Name]
[Company Name]
[Street Address]
[City, ST ZIP]
[Phone]

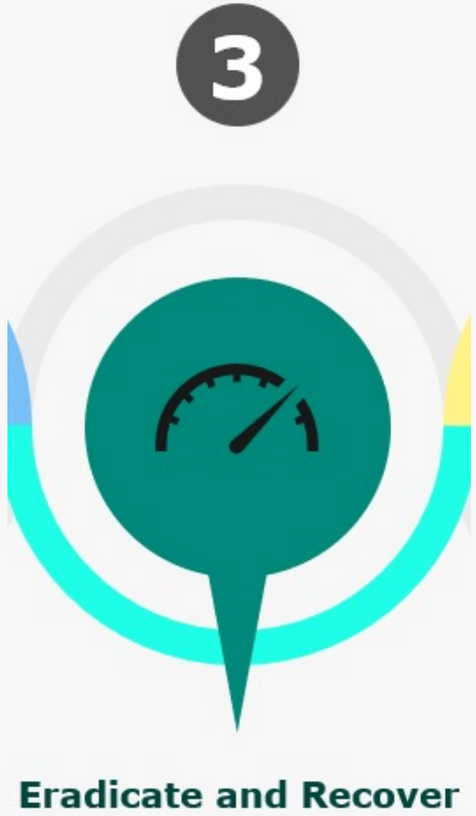
DESCRIPTION	TAXED	AMOUNT
[Service Fee]		230.00
[Labor: 5 hours at $75/hr]		375.00
[Parts]	X	345.00

Newport Consulting
Powerful Insights & Expertise

Eradicate & Recover

IT Validates that the Immediate Risk is Removed and Recovery Begins

- IT validated that there were no additional suspicious logins to other Finance team accounts, as well as no other correspondence with clients that resulted in payment information being exchanged
- IT validated that all employee passwords were reset
- IT and Management accelerated plan to implement MFA on the Office 365 environment –
  - MFA was implemented companywide within 72 hours of the breach
- IT isolated the login to access from a foreign country with no personnel with access times primarily outside of normal business hours
- Finance and IT deemed that there were no significant disclosure issues or leaks of information from the Sharepoint and OneDrive access that would cause future impact



Newport Consulting

Powerful Insights & Expertise

Impact and Root Cause Assessment

Newport Consulting
Powerful Insights & Expertise

Impact Assessment

Management Assessment of the Total Impacts

- Total impact was confirmed to be one erroneous payment instruction being executed in the amount of $250k USD
- Payment made to the erroneous account in another company's name
- Access to documents was deemed immaterial as this employee could not access sensitive company information
- The customer was a key client, thus the working relationship was seriously impacted
- Legal departments reported the incident to local police, but funds were not recovered as in the two weeks that had elapsed, the funds had been moved out of the country. Those perpetrating the crime were never caught
- Insurance company refused to reimburse the loss under the cyber policy as the email came from a legitimate company email. The deductible was roughly the same amount as the loss, so the company determined it best not to escalate this matter

Newport Consulting
Powerful Insights & Expertise

Root Cause Analysis

Root Cause Analysis

- The company did not have the proper logical security controls in place to prevent the unauthorized access
- The company did not have the proper monitoring of the environment and user accounts to identify the odd hours access from far outside the employees working area
- The company did not have the proper security awareness training as the employee voluntarily disclosed this information
- The company did not communicate controls required of its clients to prevent unauthorized payments
- The company did not have the proper coverage for its cyber insurance policy. Additionally, the deductible was far too high to be of practical use in this type of loss situation

Newport Consulting

Powerful Insights & Expertise

Control Review & Implementation

Newport Consulting
Powerful Insights & Expertise

Control Review - Internal

New internal controls were assessed and implemented into the environment

- MFA was enabled and stronger password minimum requirements were implemented
- The spam filtering was enhanced via moving to a higher Microsoft enterprise license and configuring stricter filtering.
    - More emails were now subject to rejection or quarantine automatically, thus limiting the number of phishing attempts making it to end users
- IT reviews login information periodically to determine if there are out of normal business hours or area logins – Automated solutions will be considered here
- A third-party security firm was contracted to do a live two-hour IT risk and awareness training, followed by robust recorded trainings to reinforce the message
- The company did not require controls of its clients to prevent an unauthorized payment
- The company started an external review to find a more inclusive cyber insurance policy at a more reasonable deductible level to prevent against smaller, but still material, losses

Newport Consulting
Powerful Insights & Expertise

Control Review - External

New internal controls demanded of the company's clients to continue the business relationship

- The company sent a communication to all clients requiring them to call and verify any proposed payment account or amount changes with the company analyst over the phone prior to processing, due to increases in cyber theft and hacking activity
- The company indicated that they would hold clients responsible for any payments made to a newly modified account without a call to a company analyst over the phone to validate the change prior to processing the payment. This communication will be followed-up by an email to confirm the time and nature of the call

Newport Consulting

Powerful Insights & Expertise

Outlook & Survey

Newport Consulting
Powerful Insights & Expertise

Breaches & MFA Adoption

- Microsoft spoke at a RSA security conference in 2020 and disclosed
  - In Office 365, roughly .5% of all accounts get compromised each month. This is a fascinating and disturbingly high number
  - For all enterprise Office 365 accounts, only 11% had MFA enabled as a January 2020. We believe this number is likely higher now as people moved to work remote, but this baseline number is also surprisingly low for enterprise accounts
  - Most successful account breaches occurred after simplistic attacks:
    - Taking known usernames and guessing easy passwords until they succeed
    - Use credentials for users leaked from another source and trying them at their company username as up to 60% of users are known to reuse passwords

Link:

https://www.zdnet.com/article/microsoft-99-9-of-compromised-accounts-did-not-use-multi-factor-authentication/#:~:text=Speaking%20at%20the%20RSA%20security,stops%20most%20automated%20account%20attacks

Newport Consulting

Powerful Insights & Expertise

Thank you

 | www.thenewportconsulting.com

 | contactus@thenewportconsulting.com

 | linkedin.com/company/newport-consulting-llc