RUSKIN MOSCOU FALTISCHEK P.C.
Smart Counsel. Straight Talk.

Anatomy of a Data Breach

June 7, 2023

Custom Computer Specialists
Right People. Right Results.®

Presenters

Dennis O'Connell
Director of Security Solutions
Custom Computer Specialists

Andrew T. Garbarino
Of Counsel
Ruskin Moscou Faltischek, P.C.

RUSKIN MOSCOU FALTISCHEK P.C.
Smart Counsel. Straight Talk.

Custom Computer Specialists
Right People. Right Results.®

Cooper & Schmitt, Inc.

RUSKINMOSCOUFALTISCHEK P.C.
Smart Counsel. Straight Talk.

Custom Computer Specialists
Right People. Right Results.®

Cooper & Schmitt, Inc.

- Cooper & Schmitt is a privately-held motorcycle helmet manufacturer.
- The company is a medium-sized company with approximately 500 users across 5 sites, all within the United States.
- The company has approximately 300 servers and 1,100 devices and employs an IT Staff of 3 people.
- Users continue to work in a hybrid model and have not fully returned to the office.

RuskinMoscouFaltischek P.C.
Smart Counsel. Straight Talk.

Custom Computer Specialists
Right People. Right Results®

First Contact

- At 8:30 a.m., Helpdesk receives the first calls from end-users indicating that systems – including email, financial and file shares – could not be accessed.
- Members of the IT team immediately began troubleshooting, initially believing the incident to be an internet connectivity issue and opened case with **ISP**.
- 6 hours later, it was determined that it was not an internet-related issue and was advised to examine the Company's servers
- For the next several hours, systems continued to go offline and, at 11:00 p.m., it was determined that there was an issue with the servers

Thursday
(DAY 1)

RUSKINMOSCOUFALTISCHEK P.C.
Smart Counsel. Straight Talk.

Custom Computer Specialists
Right People. Right Results.®

Ransom Note Discovered

- On Friday morning, a ransomware note is discovered on the desktops of employees.
- The note demands 72 bitcoins (approximately, $2,000,000) for the return of the data.
- Additionally, the note threatens release of the data onto the dark web if the ransom is not paid.
- Executive Management is notified of a potential cyber issue.
- Management contacts legal counsel and cybersecurity insurance company.

Friday
(DAY 2)

RUSKINMOSCOUFALTISCHEK P.C.
Smart Counsel. Straight Talk.

Custom Computer Specialists
Right People. Right Results.®

Data Incident Declared

- An Internal Incident Response Team is dispatched immediately to assess the environment.
- A cybersecurity consultant advises client to disconnect Internet connections, all networked devices and any connections to remote sites.
- The team develops a Communication Plan and begins maintenance of a timeline relating to the incident for use by counsel.
- The process for documenting findings and activities is reviewed and approved by management and counsel.

Friday
(DAY 2)

Detection and Analysis

- Initial assessment of damage: All servers have been encrypted, including 3 backups (on-premise, DR site and cloud-based).
- No useable copies of system configurations exist.
- Preliminary forensics are initiated at direction of counsel.
- All connectivity to the site is terminated.

Friday
(DAY 2)

Third Party Assistance

- Interview protocols are outlined and a list of necessary employee interviews is developed.
- A forensic firm begins in-depth analysis in conjunction with Incident Response Team.
- New networks are created in order to conduct forensic analysis (including "**clean**", "**dirty**", "**quarantined**" and "**sandbox**").
- Endpoint detection software is installed on all systems.
- Forensic analysts begin searching for **Indicators of Compromise** (IoCs):
  - Copies of systems are captured for review;
  - Work is done to trace Threat Actor's steps and activity;
  - Review of log files on systems and firewalls.

Saturday
(DAY 3)

RuskinMoscouFaltischek P.C.
Smart Counsel. Straight Talk.

Custom Computer Specialists
Right People. Right Results.®

Containment

- Cooper and Schmitt engages threat actor by requesting samples of data to confirm validity; the data is real; the ransom is $2m
- Emergency internet connection brought online for investigation and restoration.
- Rumors start to spread throughout the organization and information is leaked to the press that there was a cyber attack and data breach.

Sunday
(DAY 4)

RUSKINMOSCOUFALTISCHEK P.C.
Smart Counsel. Straight Talk.

Custom Computer Specialists
Right People. Right Results®

Eradication

- Forensic evaluation determines the **Threat Actor** (“TA”) is a known organization called “Black Cat/Alph V”.
- The TA gained access through a phishing email 6 months prior, and dropped a **payload** called “Build.exe” onto the network that sat dormant for 5 months.
- The TA **brute-forced** its way into an account with administrator privileges.
- The TA accessed the Company’s active directory and ran “ADBuild.exe”, pulling all account information, credentials, directory structure, etc.
- The TA connected to virtual environment, began encrypting all servers and deleted backups local to the data center and cloud and encrypted the backup in DR location.
- The TA connected to financial server, installed “Getmefile.exe” and exfiltrated all payroll, purchasing, accounts payable, receivables and personnel information.

Sunday through Wednesday
(DAYS 4-7)

RUSKINMOSCOUFALTISCHEK P.C.
Smart Counsel. Straight Talk.

Custom Computer Specialists
Right People. Right Results.®

Recovery

- Production data on current backup servers is deemed unrecoverable.
- Decision is made by Executive Management to not pay ransom.
- Company tells all consultants to focus on rebuild/restoration.

DAYS (5-30)

RuskinMoscouFaltischek P.C.
Smart Counsel. Straight Talk.

Custom Computer Specialists
Right People. Right Results.®

Now What?

RUSKINMOSCOUFALTISCHEK P.C.
Smart Counsel. Straight Talk.

Custom Computer Specialists
Right People. Right Results.®

What Made This Organization Vulnerable?

- Lack of employee training;
- Systems that could not be patched;
  - other patching not up to date;
- Firewall was not running IPS/IDS or had geo-blocking configured;
- Did not utilize multi-factor authentication;
- Ran standard anti-virus but not EDR solution;
- Did not have an air-gapped backup solution;
- Did not implement an Incident Response Plan.

RuskinMoscouFaltischek P.C.
Smart Counsel. Straight Talk.

Custom Computer Specialists
Right People. Right Results.®

Questions and Answers