GBQ

Navigating Cyber Considerations Beyond PCI Compliance

July 18, 2023

Presenters

Dustin Minton, CPA, MBA
Director, Assurance &
Business Advisory Services
513.744.5073
dminton@gbq.com

Doug Davidson, CISA
Director of Information
Technology Services
614.947.5340
davidson@gbq.com

Ray Tefft
Senior Manager of
Cybersecurity
614.947.5341
rtefft@gbq.com

Eric Mason
Senior Security
Analyst
614.947.5308
EMason@gbq.com

Agenda

- Welcome
- Introductions
- NCR Ransomware Case Study
- Beyond PCI
  - Restaurant Cyber Risks
  - Ransomware
  - Awareness
  - Web Site
- Protect Yourself
  - Framework for Success
  - Cyber Liability Insurance
  - Security Scorecard
- Questions

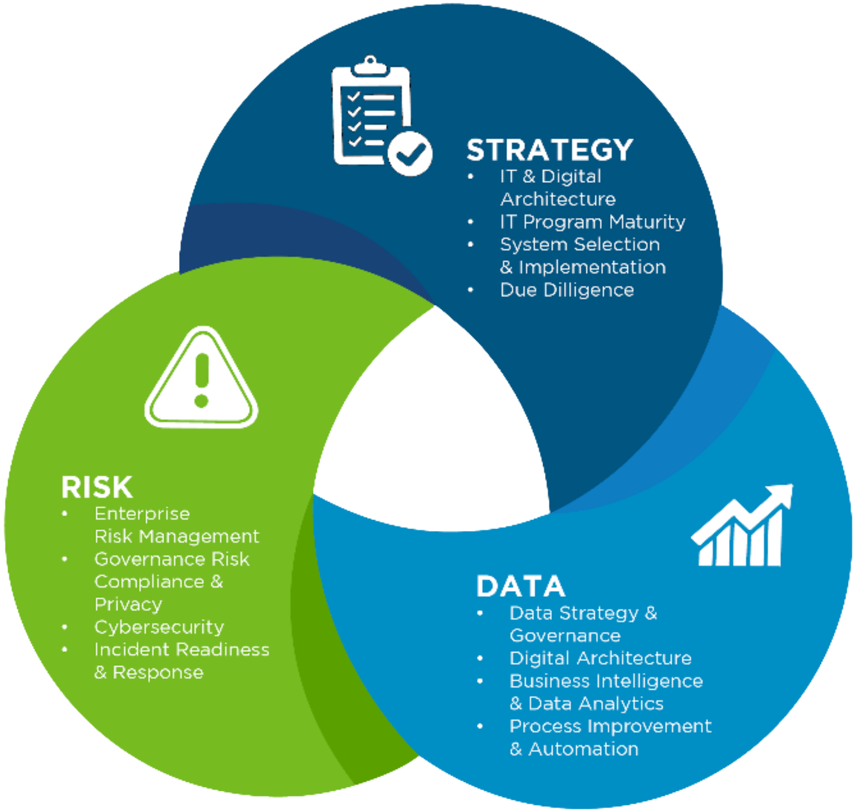
Save The Date

- August 15th: Mastering Lease Accounting - A Recipe for Restaurant Success Webinar
- October 24th: Columbus Restaurant MasterClass All-Day Seminar
- November 9th: Unveiling Data-Driven Insights for Success Webinar

Visit us online to watch past Restaurant MasterClass webinar recordings.

Introducing GBQ Technology Services

We maximize technology and data investments while building trust and keeping the bad guys out by helping clients answer 3 key questions:



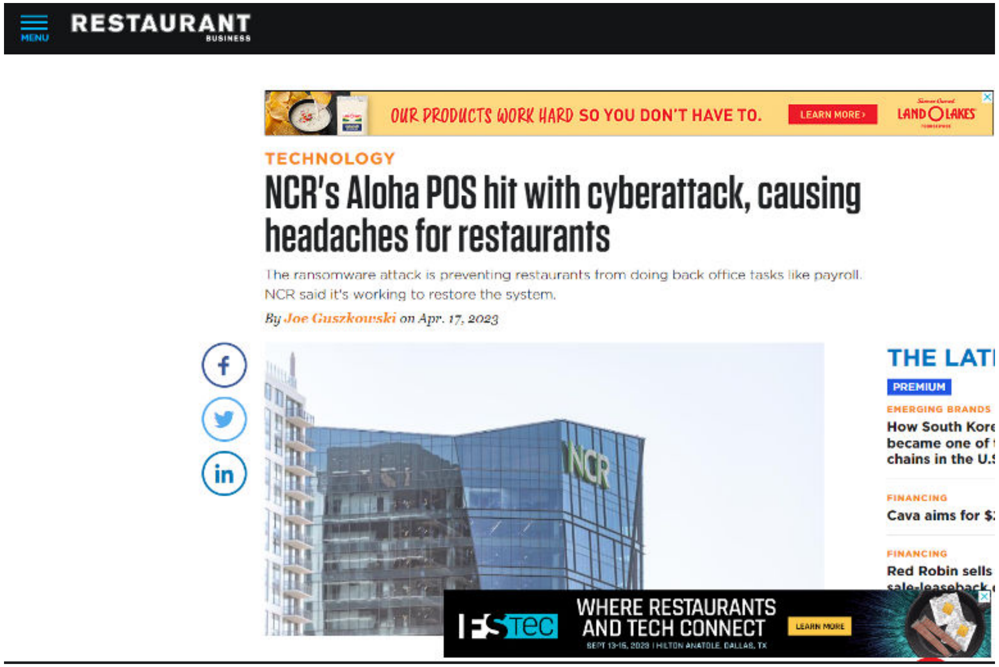
STRATEGY
- IT & Digital Architecture
- IT Program Maturity
- System Selection & Implementation
- Due Dilligence

RISK
- Enterprise Risk Management
- Governance Risk Compliance & Privacy
- Cybersecurity
- Incident Readiness & Response

DATA
- Data Strategy & Governance
- Digital Architecture
- Business Intelligence & Data Analytics
- Process Improvement & Automation

- **Strategy** – Is IT aligned with and serving the business?
- **Risk** – Are enterprise, compliance, cyber and other risks managed within management's tolerance?
- **Data** – Does the business have the right data in the right form to run and grow?

NCR Ransomware: Case Study in Third-Party Risk



TECHNOLOGY

NCR's Aloha POS hit with cyberattack, causing headaches for restaurants

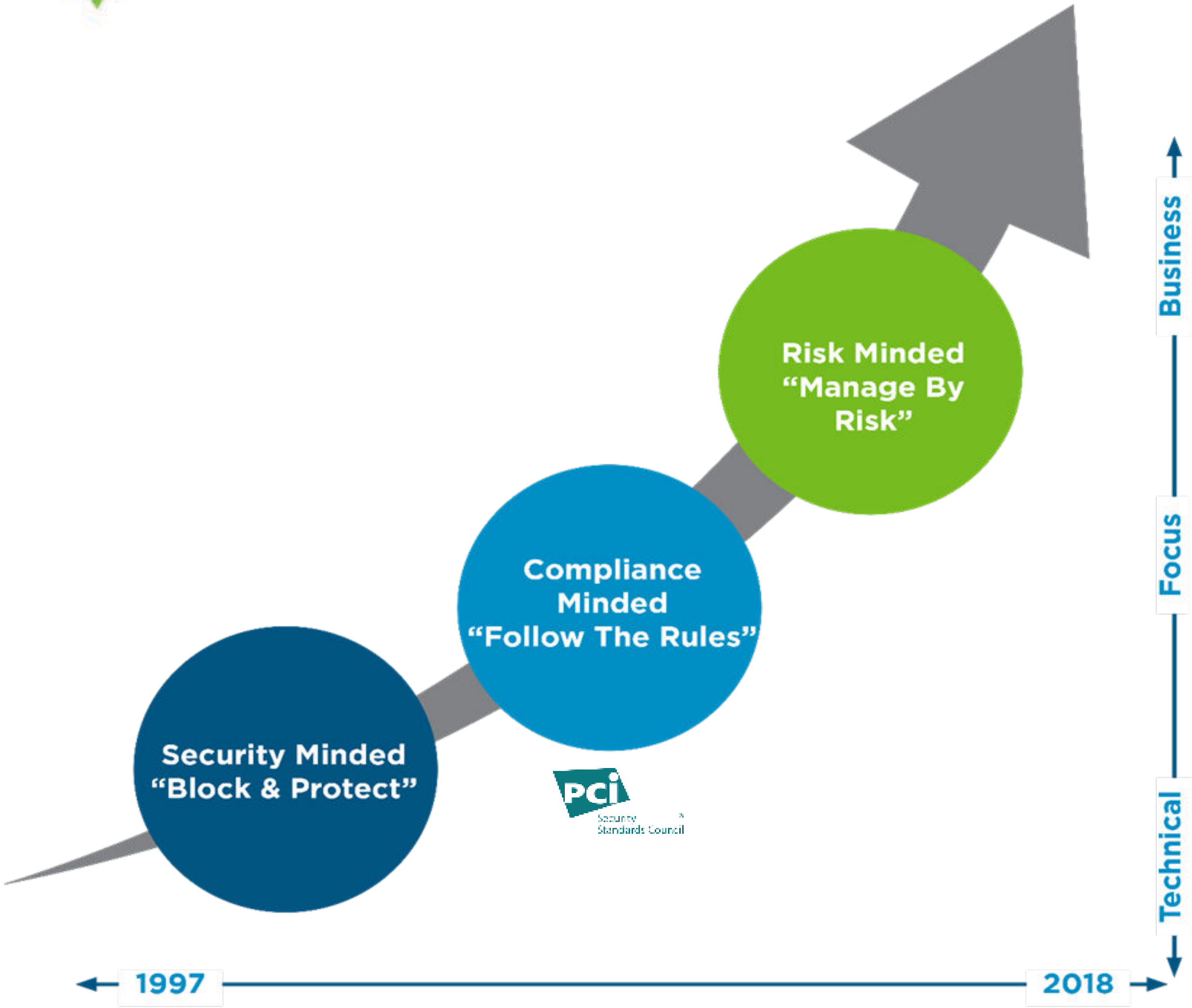
The ransomware attack is preventing restaurants from doing back office tasks like payroll. NCR said it's working to restore the system.

By Joe Guszkowski on Apr. 17, 2023

Lessons:

- ✓ Every firm, no matter the size, is susceptible to ransomware.
- ✓ Restaurants must manage the risk that company owned systems are at risk of being ransomed and should take measures to reduce that risk.
- ✓ As restaurants outsource key functionality, like point-of-sale systems, inventory, scheduling, gift card and other loyalty programs, delivery services, accounting, IT managed services, marketing and so on, a program should be in place to measure and manage the risks that exist from those key third parties.

Focus of Cybersecurity Management Over Time



Security Minded
"Block & Protect"

Compliance Minded
"Follow The Rules"

PCI Security Standards Council

Risk Minded
"Manage By Risk"

1997

2018

Technical

Focus

Business

- Security Minded Phase was about "keeping them out"

- Compliance Minded Phase was about "checking the box" (PCI)

- Risk Minded Phase is about measuring and managing risk to build resiliency

PCI Data Security Standard

PCI Security Standards Council

- Information security standard used to handle credit cards from major brands.
- Use by Merchants is mandated by the card brands
- Validation of compliance is performed annually or quarterly with a method suited to the volume of transactions.
- Focused on a Merchant's (Restaurant) Cardholder Data Environment

Build and maintain a securenetwork and systems

Protect cardholder data

Maintain a vulnerability management program

Implement strong access-control measures

Regularly monitor and test networks

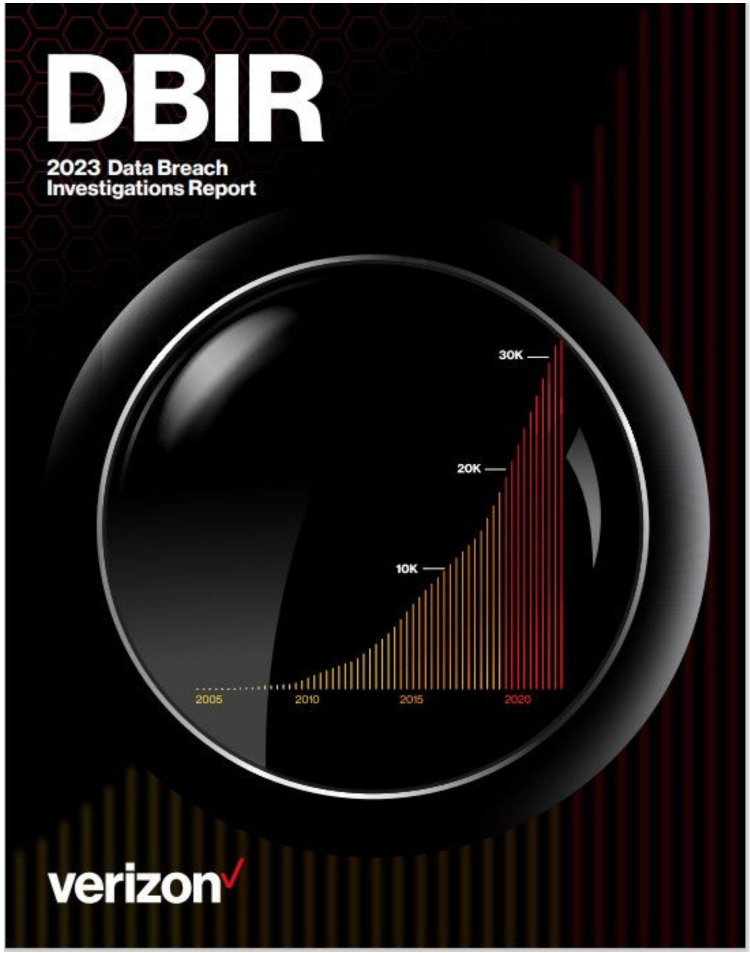
Maintain an information security policy

What Assets Are Not in Your Cardholder Data Environment?

Not specifically covered by PCI DSS:

- Back Office Operations
- Front of Store
- Back of Store
- Third Party Systems
- Internet Connected Automation Systems

What Are Our Threats? - Verizon "DBIR"



- Verizon Data Breach Investigation Report
- Established 2008
- Data Driven Report of Incidents and Breaches

Social Engineering on the Rise

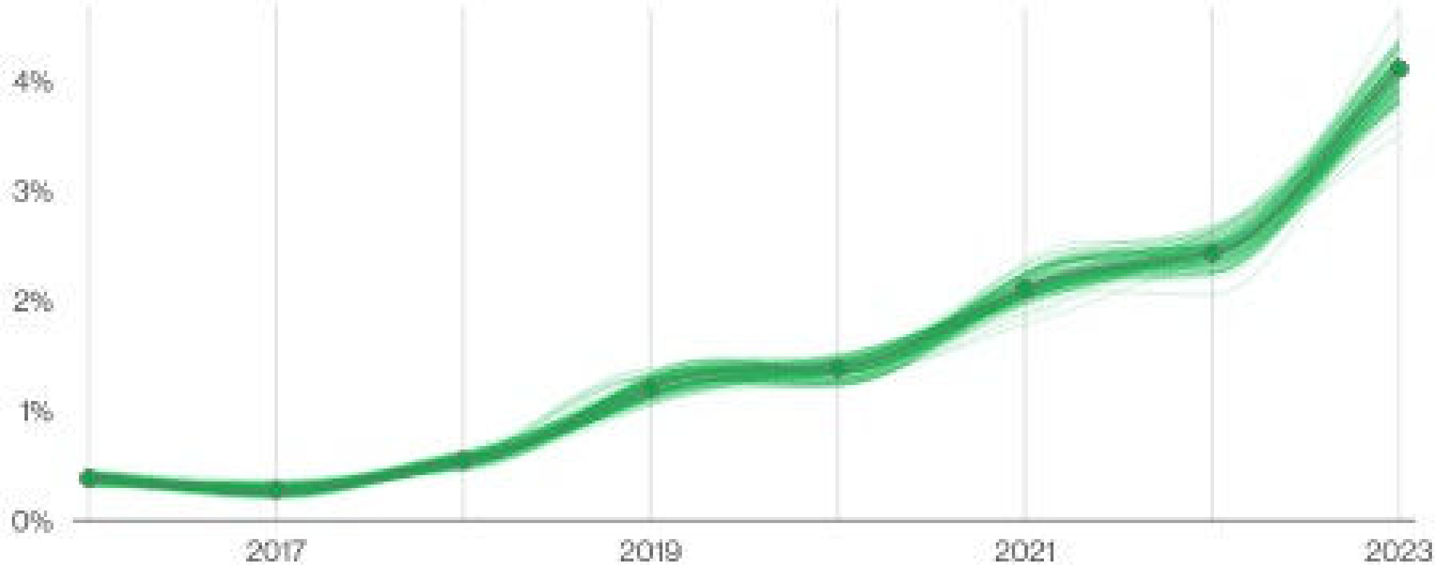


Figure 5. Pretexting incidents over time

DBIR Report 2023 - Introduction | Verizon Business

Ransomware 24% of All Breach Events

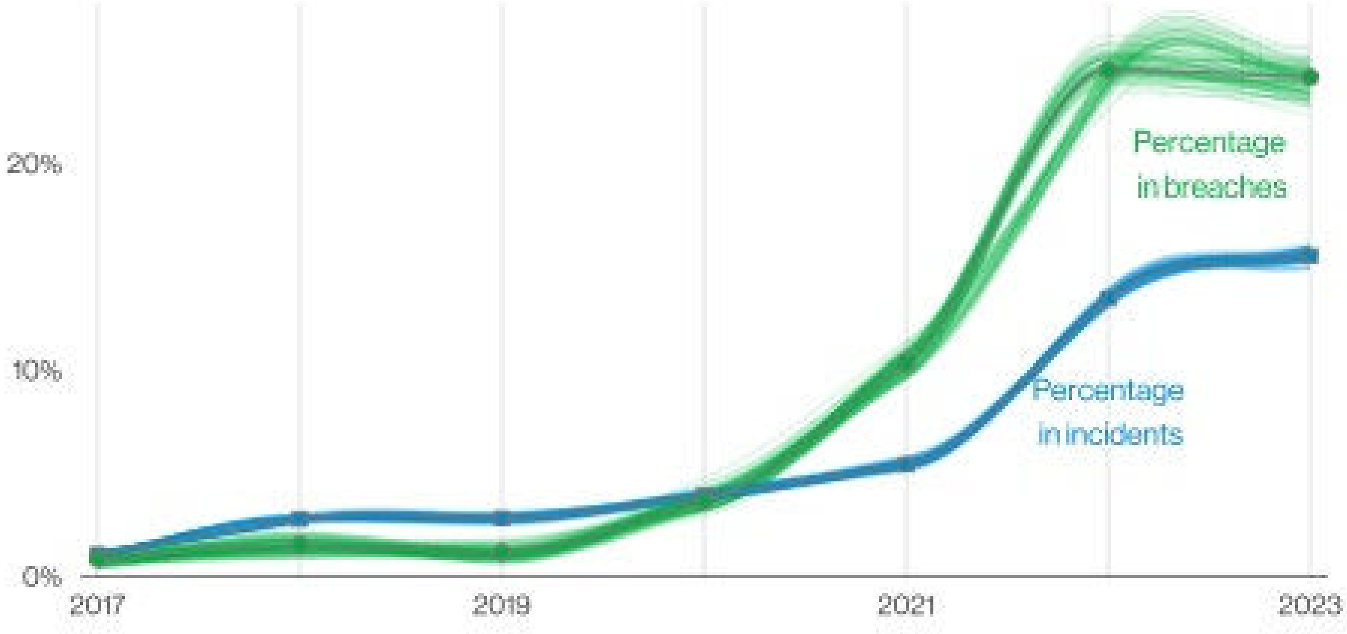


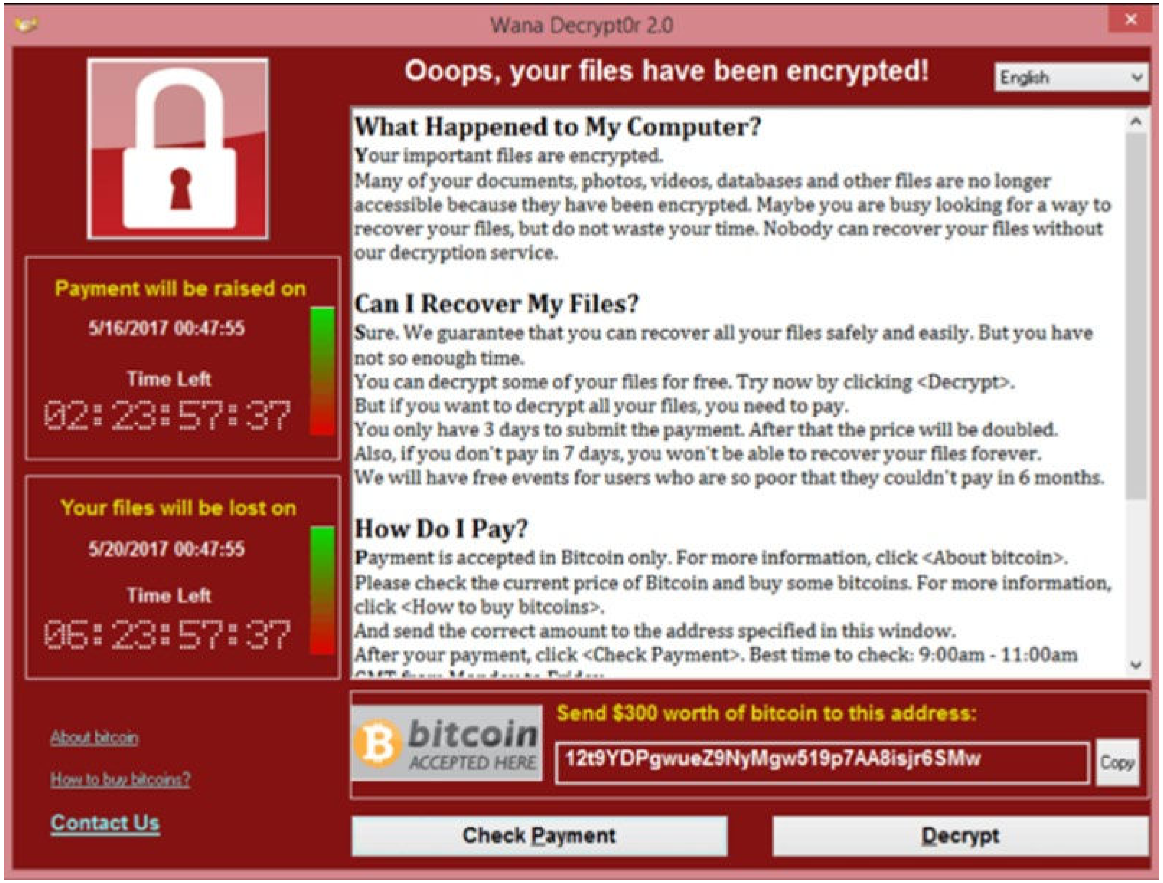
Figure 8. Ransomware action variety over time.

[DBIR Report 2023 - Introduction | Verizon Business]

By Industry Sector

Metric	Accommodation & Food Services	Retail	SMB
Frequency	406 incidents 193 breaches	254 incidents 68 breaches	699 incidents 381 breaches
Top patterns	88% of breaches: System Intrusion Social Engineering Basic Web Attacks	90% of breaches: System Intrusion Basic Web Attacks Social Engineering	92% of breaches: System Intrusion, Social Engineering Basic Web Attacks
Threat actors (breaches)	External (94%), Internal (7%) Multiple (2%) Partner (2%)	External (93%) Internal (9%) Multiple (1%)	External (94%) Internal (7%) Multiple (2%) Partner (1%)
Actor motives (breaches)	Financial (100%), Espionage (1%)	Financial (100%)	Financial (98%) Espionage (1%) Convenience (1%) Grudge (1%)
Data compromised (breaches)	Payment (37%) Credentials (35%) Other (32%) Personal (23%)	Payment (41%), Credentials (38%) Personal (34%) Other (26%)	Credentials (54%) Internal (37%) Other (22%) System (11%)

Ransomware



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

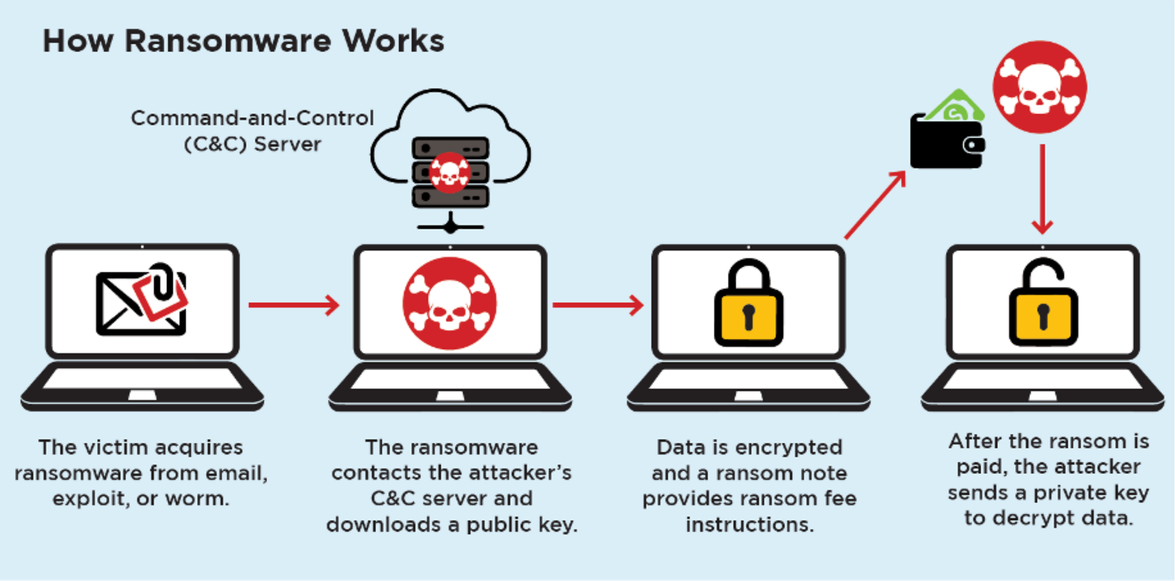
Screenshot of the ransom note left on an infected system

Ransomware is a type of malicious code or software that attackers use to gain control over your computer and files.

The attackers lock up your computer and demand a ransom in exchange for providing you with the decryption key to allow you to regain access to your computer and files.

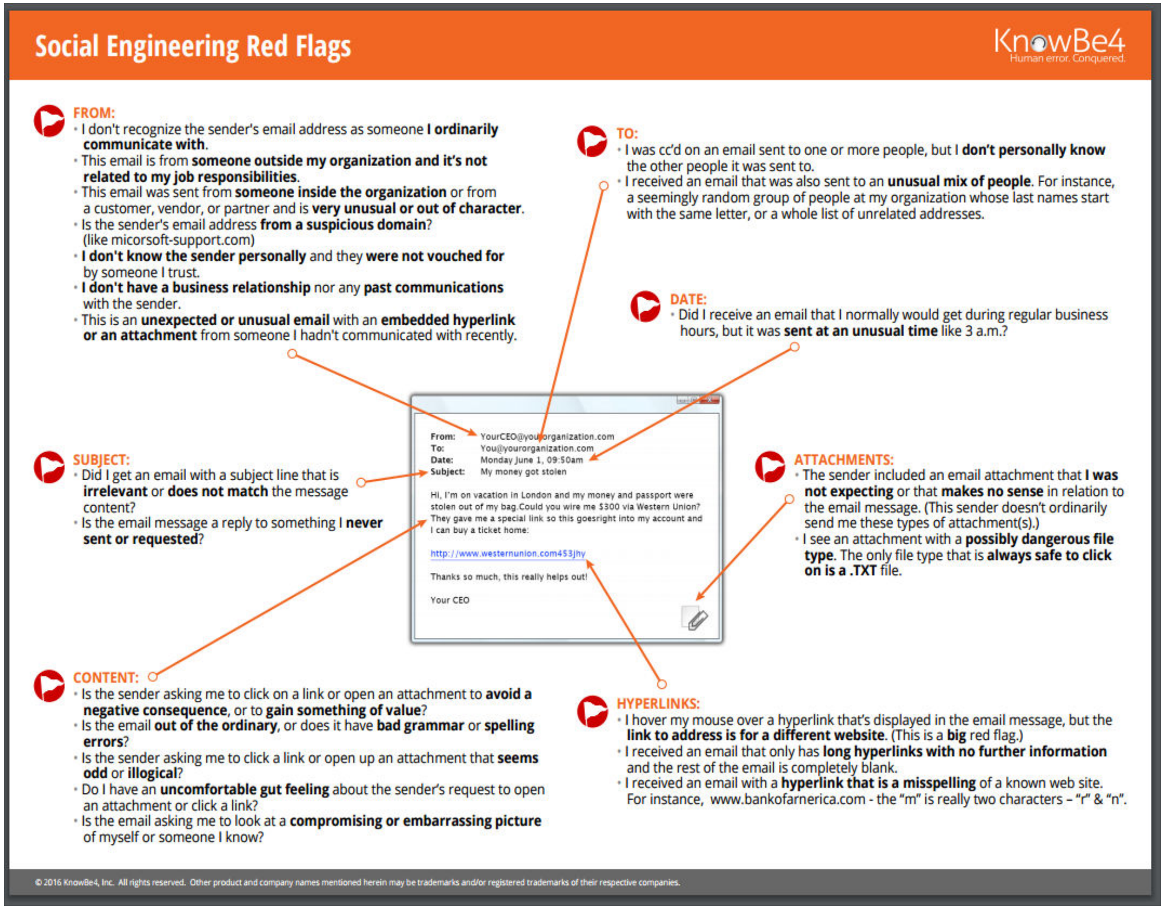
Paying the ransom does not always guarantee you access to your computer and files and could make you a victim of further attacks.

Defending Against Ransomware


How Ransomware Works
Command-and-Control (C&C) Server
The victim acquires ransomware from email, exploit, or worm.
The ransomware contacts the attacker's C&C server and downloads a public key.
Data is encrypted and a ransom note provides ransom fee instructions.
After the ransom is paid, the attacker sends a private key to decrypt data.

- Trust but verify your cybersecurity program with an annual assessment and security testing including ransomware simulation
- Backup your data (and test restoration)
- Train employees to raise security awareness
- Have a written, tested incident response plan
- Ensure you have the right cyber insurance coverage

Social Engineering



Social Engineering Red Flags

KnowBe4
Human error. Conquered.

FROM:
- I don't recognize the sender's email address as someone **I ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address **from a suspicious domain**? (like micorsoft-support.com)
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any **past communications** with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I hadn't communicated with recently.

TO:
- I was cc'd on an email sent to one or more people, but I **don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, a seemingly random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

DATE:
- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT:
- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something I **never sent or requested**?

From: YourCEO@yourorganization.com
To: You@yourorganization.com
Date: Monday June 1, 09:50am
Subject: My money got stolen

Hi, I'm on vacation in London and my money and passport were stolen out of my bag.Could you wire me $300 via Western Union? They gave me a special link so this goesright into my account and I can buy a ticket home:

http://www.westernunion.com453jhy

Thanks so much, this really helps out!

Your CEO

ATTACHMENTS:
- The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me these types of attachment(s).)
- I see an attachment with a **possibly dangerous file type**. The only file type that is **always safe to click on is a .TXT** file.

CONTENT:
- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence**, or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

HYPERLINKS:
- I hover my mouse over a hyperlink that's displayed in the email message, but the **link to address is for a different website**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information** and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com - the "m" is really two characters – "r" & "n".

- Train employees to raise security awareness
- Implement strong internal financial controls focused on banking, payments & employee compensation
- Ensure PCI Cardholder Environment employees receive proper information handling training

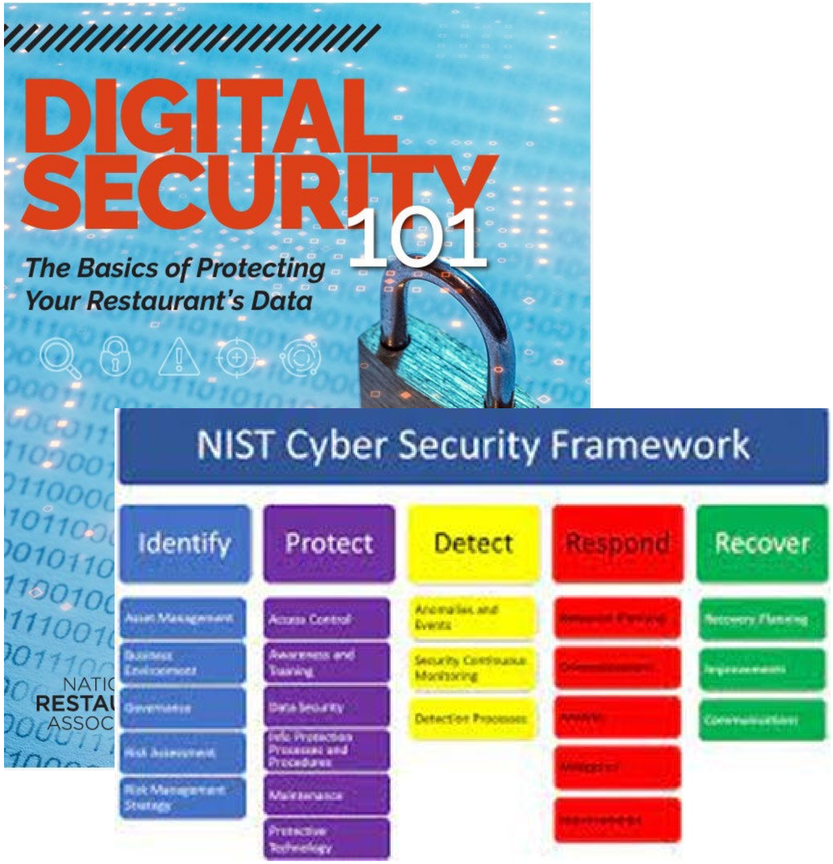
Web Site Risks

- Skimmers (RAM Scrappers) -- Malware injected into a site that "skims" data from card transactions
- Authorization Schemes – stolen payment card numbers are authorized on your storefront as bad actors work to find working CVV codes for the cards
- ADA Compliance - Non-compliant sites attract the attention of attorneys
- Brand Damage - Defacements & customer focused attacks

Defending Your Web Site

- Identify which party (Marketing, IT, Third Party Developer, Third Party Hosting Provider) is responsible for which components of security
- Ensure these roles are contractually obligated for third parties and documented in policy for internal actors
- Include all parties in your written incident response plan
- Utilize a third-party cyber security expert to identify security vulnerabilities

Manage Security From a Playbook


DIGITAL SECURITY 101
The Basics of Protecting Your Restaurant's Data
NATIONAL RESTAURANT ASSOCIATION

NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

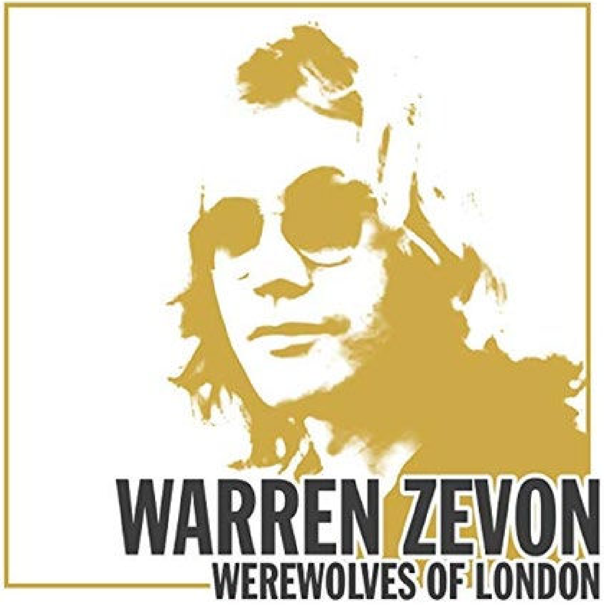
National Institute for Standard & Technology's Framework for Improving Cybersecurity in Critical Infrastructure (NIST Framework):

1. Identifying cyber risks;
2. Protecting against cyber risks;
3. Setting up procedures to detect a cyber-incident;
4. Responding to a cyber-incident; and
5. Recovering from a breach

Intro to Digital Security 101: How to protect your restaurant's data | National Restaurant Association

Cyber Liability Insurance

- ✓ Review annually with a broker with cyber knowledge and experience
- ✓ Riders on property & casualty are often not enough
- ✓ Accurately complete underwriting forms
- ✓ Understand how much coverage you need
- ✓ Understand type of coverages.



"Send lawyers, guns and money. Dad get me out of this."
 - Warren Zevon,
 Lawyers, Guns and Money,
 Werewolves of London

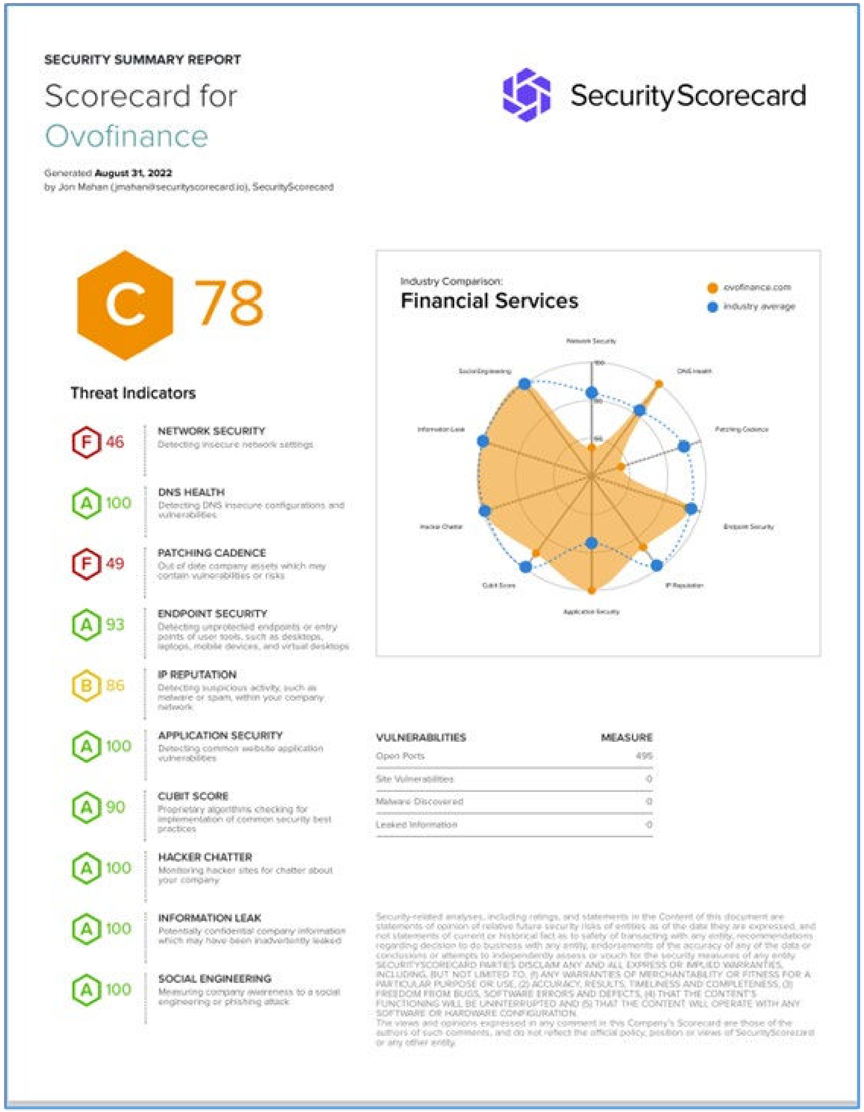
Security Scorecard

Companies use cyber-risk ratings services such as those offered by BitSight and Security Scorecard to assess the security risk posed by vendors / supply chain.

Insurance carriers are using in underwriting processes.

Many of these risk ratings services will provide free copies of your report to you.

Obtain reports on your company to see what your score is and fix any weaknesses



SECURITY SUMMARY REPORT

Scorecard for
Ovofinance

SecurityScorecard

Generated **August 31, 2022**
by Jon Mahan (jmahan@securityscorecard.io), SecurityScorecard

C 78

Threat Indicators

F 46 — **NETWORK SECURITY**
Detecting insecure network settings

A 100 — **DNS HEALTH**
Detecting DNS insecure configurations and vulnerabilities

F 49 — **PATCHING CADENCE**
Out of date company assets which may contain vulnerabilities or risks

A 93 — **ENDPOINT SECURITY**
Detecting unprotected endpoints or entry points of user tools, such as desktops, laptops, mobile devices, and virtual desktops

B 86 — **IP REPUTATION**
Detecting suspicious activity, such as malware or spam, within your company network

A 100 — **APPLICATION SECURITY**
Detecting common website application vulnerabilities

A 90 — **CUBIT SCORE**
Proprietary algorithms checking for implementation of common security best practices

A 100 — **HACKER CHATTER**
Monitoring hacker sites for chatter about your company

A 100 — **INFORMATION LEAK**
Potentially confidential company information which may have been inadvertently leaked

A 100 — **SOCIAL ENGINEERING**
Measuring company awareness to a social engineering or phishing attack

Industry Comparison:
Financial Services

VULNERABILITIES	MEASURE
Open Ports	495
Site Vulnerabilities	0
Malware Discovered	0
Leaked Information	0

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.
The views and opinions expressed in any comment in this Company's Scorecard are those of the authors of such comments, and do not reflect the official policy, position or views of SecurityScorecard or any other entity.

Questions

We Want to Hear from You!

Share your feedback from today's presentation here:

Contact Information

Dustin Minton, CPA, MBA
Director, Assurance & Business Advisory Services
513.744.5073
dminton@gbq.com

Doug Davidson, CISA
Director of Information Technology Services
614.947.5340
davidson@gbq.com

Ray Tefft
Senior Manager of Cybersecurity
614.947.5341
rtefft@gbq.com

Eric Mason
Senior Security Analyst
614.947.5308
EMason@gbq.com