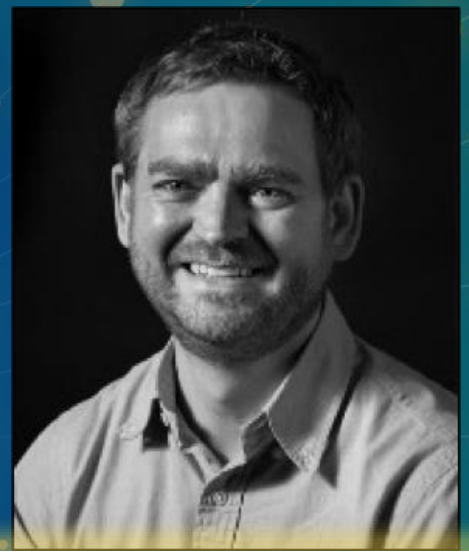
PCI Security Standards Council

You've Been Hacked!

Now What?

You Been Hacked Guides

Who we are



online business systems

Robert C Harvey Jr., *CISSP*
Managing Director
Risk, Security and Privacy

p 678.792.0205
m 404.452.7452
rharvey@obsglobal.com

obsglobal.com
Atlanta, GA

PCI Security Standards Council

online business systems

Adam Kehler, *CISSP*
Director, Healthcare
Cybersecurity Services
Risk, Security and Privacy

m 785. 727. 0922
akehler@obsglobal.com

obsglobal.com
Lancaster, PA

Agenda

- Who We Are
- Learning Objectives
- PCI DSS v4.0 r12.10.1 Discussion
- YOU BEEN HACKED
- NOW WHAT?
- Recommendation Roadmap
- Closing Thoughts

online business systems

Who we are

Founded in 1986
Privately held

Over 400 professionals in USA, Canada and EMEA

Working with Clients around the globe

"We know that when great people, who share a set of common values, work together, they can accomplish great things."

– Chuck Loewen
President and Chief Executive Officer

Cybersecurity

- Assessment Services
- Healthcare Services

- Advisory Services
- Technical Security Services
- Salesforce
- Cloud Solutions

Digital Transformation

- Digital Advisory Services
- Customer Experience

- Digital Studio
- Service Management

"I have forty-eight information technology vendors and just one partner, and that is Online."

– James Nick
Director, PMO

17 consecutive years on Best Workplaces

65 NPS against an Industry average of 41

4.7 Company Rating On Glassdoor

99% CEO Approval rating on Glassdoor

Learning Objectives

1. Gain practical recommendations on handling the first steps after an incident is declared to strengthen the maturity of your cybersecurity program to go above and beyond the PCI Security Standards.

2. Do you know what you're going to say? In this session, we will provide some insights on Crisis Communication. Internal messaging is as important as external.

3. Learn proactive ways to create the best possible outcomes of the declared incident. Key steps on getting a clean bill of health to return back to normal operations.

PCI DSS v4.0 Requirement 12.10.1

12.10.1 An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident. The plan includes, but is not limited to:

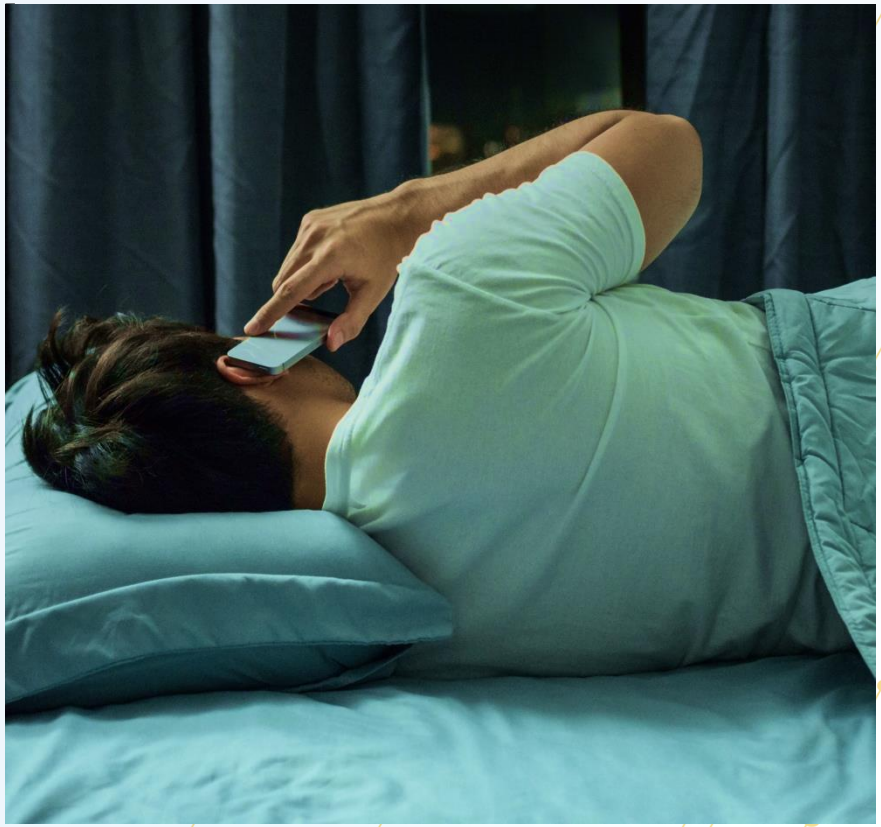
- Roles, responsibilities, and **communication and contact strategies** in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum.
- Incident response procedures with specific containment and mitigation activities for different types of incidents.
- **Business recovery and continuity procedures.**
- Data backup processes.
- Analysis of legal requirements for reporting compromises.
- Coverage and responses of all critical system components.
- Reference or inclusion of incident response procedures from the payment brands.

PCI Security Standards Council

You’ve Been Hacked: Now What?

The Scenario

It's 2am and the phone rings. You've been hacked and your data is being held ransom – operations are shut down, panic is setting in, stories are circulating online via social channels, and employees are waiting for direction.



PCI Security Standards Council

Oh, Shoot!!?

What do you do?

What's your first phone call?

This interactive session will role play just what happens after that phone call. We'll cover some of the best first steps, look at response from a technical and communications viewpoint and look to the audience for ideas, how their organizations have planned for this and more.

PCI Security Standards Council

Declaring an Incident

How are you communicating?

Do you have incident declaration criteria?

How are you going to reach the incident command team and executives?

PCI Security Standards Council

Crisis Communication

What is your plan?

Do you know what you're going to say?

Do you know who you're going to say it to and how?

Do you know who is going to say it?

Can you setup out-of-band communication channels?

Do you know when to contact the payment brands?

PCI Security Standards Council

Continuing Operations

Have you tested your plan?

Have frontline workers practiced for this event?

Do you have an emergency operations plan?

How quickly can you bring up a recovery environment?

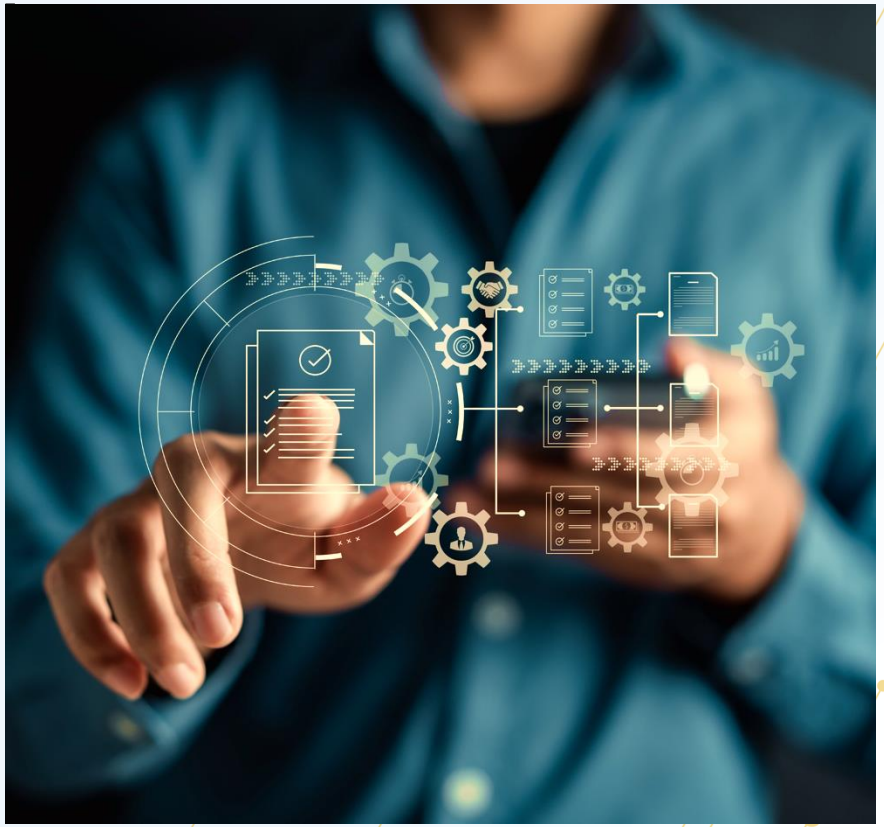
PCI Security Standards Council

Recovering

Is it safe?

When is it safe to reconnect systems?

How do you transition back from paper and downtime procedures?



PCI Security Standards Council

Ransomware Roadmap

Where to start?

What steps can you take to address the risk of attack (avoid, transfer, accept, and mitigate) and the damage that results from ransomware attacks?

PROTECT

What are the appropriate technologies and practices to take to detect ransomware attacks?

DETECT

What is the appropriate response if a ransomware is detected to reduce the impact?

RESPOND

How do you recover from the attack with the goal of:

- Minimal impact
- Adequate resources to respond
- Not paying a ransom

RECOVER

Where are you susceptible to ransomware attacks. What is your capability to restore from a ransomware attack?

IDENTIFY

Closing Thoughts

Are you prepared?

Declaring an Incident

Engaging Partners

Crisis Communications

Continuing Operations

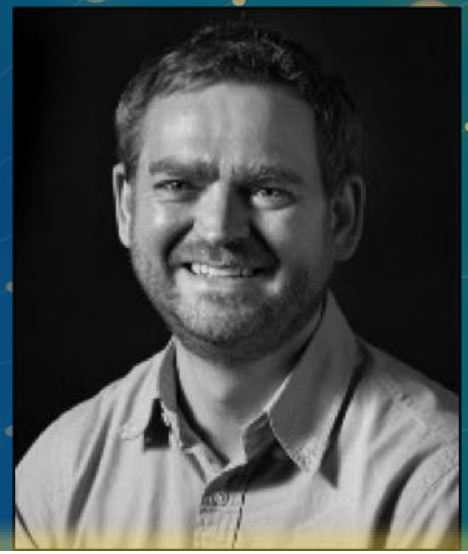
Negotiating the Ransom

Recovering

PCI Security Standards Council

Connect with us in the Vendor Showcase

REQUIREMENT 12
Security & COMPLIANCE PROGRAM



online business systems

Robert C Harvey Jr., *CISSP*
Managing Director
Risk, Security and Privacy

p 678.792.0205
m 404.452.7452
rharvey@obsglobal.com

obsglobal.com
Atlanta, GA

online business systems

Adam Kehler, *CISSP*
Director, Healthcare
Cybersecurity Services
Risk, Security and Privacy

m 785. 727. 0922
akehler@obsglobal.com

obsglobal.com
Lancaster, PA