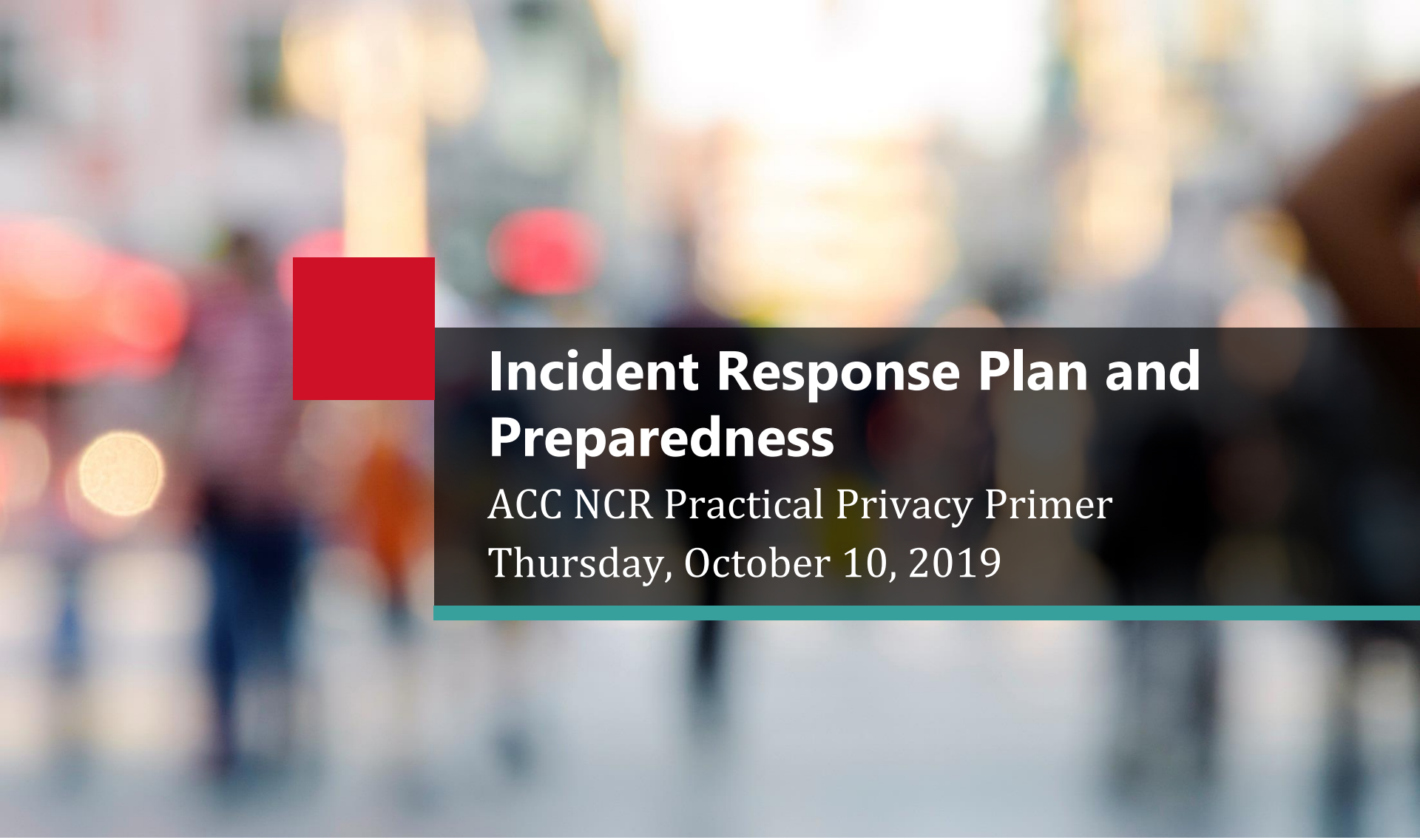


Incident Response Plan and Preparedness

ACC NCR Practical Privacy Primer

Thursday, October 10, 2019

CONFIDENTIAL
© Copyright Baker Botts 2019. All Rights Reserved.

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

BAKER BOTTS

Panelists

Erika Brown Lee
Senior Vice President & Assistant General Counsel, Mastercard

Heather Choi
Partner, Baker Botts L.L.P.
heather.choi@bakerbotts.com

Maureen Ohlhausen
Partner, Baker Botts L.L.P.
maureen.ohlausen@bakerbotts.com

Kate Weir
Director, Global Crisis Center
PwC

Audience Poll

- ❑ Do you know what a crisis is for your organization?
- ❑ Can you foresee where it may occur?
- ❑ Do you think you would recognize it in time?
- ❑ Do you have a overall plan to handle it?
- ❑ Do you have a team and reporting lines in place?
- ❑ Do you have procedures for unavailability or recusal?
- ❑ Have you done a "mock event"?
- ❑ Are you ready at the leadership and operational levels?
- ❑ Do you feel prepared to handle "the domino effect"?

98% of respondents expect to experience a crisis in the future

In the event of a crisis, would you have confidence in making decisions that would protect your strategy and the long-term fate of your company?

Would you trust your gut?

Would you trust your team?

When the spotlight is on, how would you fare?

98%

Source: PWC Global Crisis Response Survey, 2019

How Prepared are You?

49%

of organizations either **don't have someone in charge of crisis management** or have not as yet defined that person's responsibilities.

47%

of organizations either **don't have a crisis response plan** or only have a basic checklist of things to do.

21%

of organizations **do not have any crisis planning in place at all**.

25%

of respondents have a dedicated budget for crisis preparedness and **spend up to $100,000 per year or more**.

Source: PWC Global Crisis Response Survey, 2019

HYPOTHETICAL: WORRY FREE EATS

BAKER BOTTS

Worry Free Eats

You are the GC of a web-based company supplying foods free of common allergens.

On a Sunday morning, you receive a call from your lead IT team that they detected unusual amounts of outgoing traffic on your system overnight. It's stopped, but they're concerned that the system has been breached.

Your System has Been Breached

- What do you do?
- What are your initial conversations and first steps?
- What outside parties do you contact?
- What about the C-Suite?

Secure Your Operations

- Assemble a team of experts
  - Data Forensics
  - Legal Counsel
- Secure physical areas
- Stop data loss
- Remove improperly posted information from the web
- Interview people who discovered the breach
- Preserve Evidence

How did this happen?

You find out that an employee in the finance department received a phishing email and provided his login credentials.

- How can your forensics experts help find out what was accessed?
- What kind of training did you have for employees?
- What impact does/should that information have on your response strategy and narrative?

In the Matter of BLU Products and Samuel Ohev-Zion.: The FTC alleged that **defendants falsely claimed that they had implemented "appropriate" physical, electronic, and managerial procedures** to protect consumers' personal information. In fact, according to the complaint, defendants failed to implement appropriate security procedures to oversee the security practices of their service providers.
https://www.ftc.gov/enforcement/cases-proceedings/172-3025/blu-products-samuel-ohev-zion-matter

Fix Vulnerabilities

- ❑ Think about service providers
- ❑ Check network segmentation
- ❑ Work with forensics experts
- ❑ Have a communications plan

Who is impacted? Who do we have to tell?

You learn that financial information has been compromised, along with potential health data, and you're not sure if any of your European customers have been impacted.

- Do you have obligations under HIPAA?
- What steps need to be taken to identify whether it has effected your international customers? If it has, then what?

In the Matter of Paypal, Inc.: The FTC alleged that Venmo did not have a written information security program through at least August 2014, and that, until at least March 2015, **Venmo failed to notify users when their password or email address had been changed, or when a new device had been added to their account.** As a result, unauthorized users were able to withdraw funds from consumer accounts –without Venmo notifying consumers.
https://www.ftc.gov/enforcement/cases-proceedings/162-3102/paypal-inc-matter

Notify Appropriate Parties

- ❑ Determine Legal Requirements
- ❑ Notify Law Enforcement
- ❑ Determine type of data involved
  - ❑ Medical data under HIPPA
  - ❑ EU personal data under GDPR
- ❑ Notify affected businesses
- ❑ Notify individuals

What are people asking?

The allergen community and loyal customers have noticed your site is down and the press begins calling.

- How do you prepare leadership to address media inquiries?
- What information do you provide?

Now what?

You've gotten the system back up and running and the holes plugged. It's been a rough week and your mother calls to see how you're doing.

She also she tells how nice it is that your company emailed her to ask for her date of birth and social security number to enroll her in credit monitoring…

- How to identify the full scope of the breach?
- How do you manage the long-term effects?

In the Matter of Uber Technologies, Inc.: Following that announcement, the Commission learned that Uber had failed to disclose a significant breach of consumer data that occurred in the midst of the FTC's investigation that led to the 2017 settlement announcement. Due to Uber's misconduct related to the 2016 breach, Uber is now subject to additional requirements.
https://www.ftc.gov/enforcement/cases-proceedings/152-3054/uber-technologies-inc

Phase 1: Initial Considerations

- ❑ Response priorities
- ❑ Investigation – scope, approach, facts, "known unknowns," disclosures, 3rd party support
- ❑ Operational response/business impact
- ❑ Information Sharing (Internal)
  - ❑ Response team construct
  - ❑ Internal reporting/notifications
  - ❑ Board considerations
  - ❑ External auditors
- ❑ External Communications
  - ❑ Relevant stakeholders
  - ❑ Messaging – scope, approach, approvals, priorities

Phase 2: Resiliency Plan

- ❑ Strategies to emerge from the fallout
- ❑ Don't wait for case resolutions to plan for the future
- ❑ Proactively take advantage of opportunity to improve the narrative and plan for the future
- ❑ Invest in and implement plan to re-build trust and maintain important business and stakeholder relationships
  - Unaffected customers, vendors, suppliers
  - Affected customers
  - Other stakeholders
- ❑ Commit to fixing the problems and follow through
- ❑ Periodically reassess to adjust plan, as needed

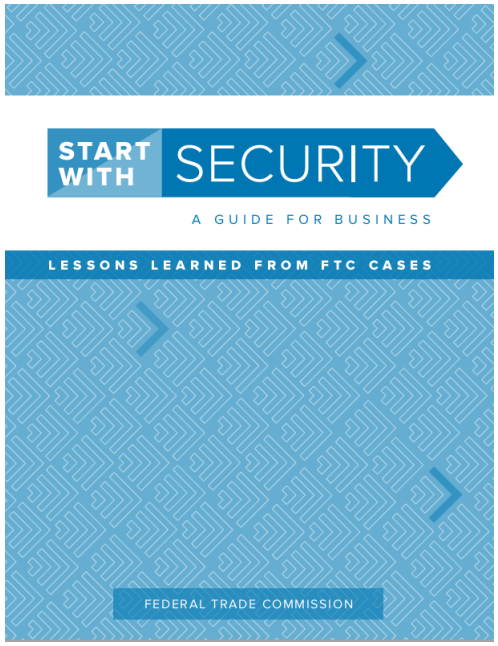
Key Take-Aways

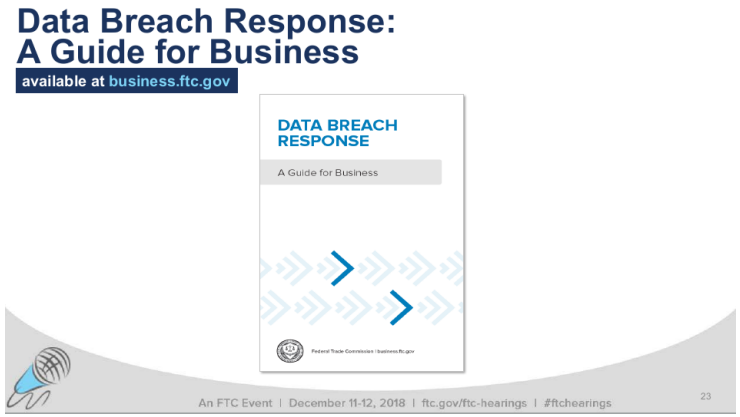
- ❑ Plan in advance but remain nimble
- ❑ Identify a decision-maker (i.e. crisis management team)
- ❑ Make sure decision-maker is independent of problem
- ❑ Speak with one voice
- ❑ Tell the truth
- ❑ Take responsibility & fix the problem
- ❑ Maintain credibility at all times – with all constituents
- ❑ Learn from missteps
- ❑ Be resilient and plan for future

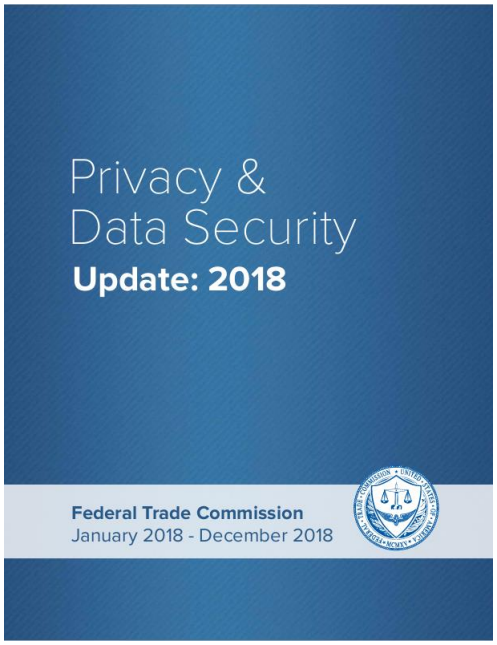
RESOURCES 02

BAKER BOTTS

FTC Data & Privacy Guides







Start with Security: https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business

Data Breach Response: https://www.ftc.gov/tips-advice/business-center/guidance/data-breach-response-guide-business

Privacy & Data Security Update: https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2018/2018-privacy-data-security-report-508.pdf

Additional Resources from the FTC

Start with Security:
Lessons Learned from FTC Cases
available at business.ftc.gov

FTC Staff Perspective:
Email Authentication
available at business.ftc.gov

Stick with Security:
An FTC Business Blog series
available at business.ftc.gov

Cybersecurity for Small Business
available at business.ftc.gov

Careful Connections:
Building Security in the Internet of Things
available at business.ftc.gov

FTC Staff Perspective:
Web Hosts
available at business.ftc.gov

Educational Videos for Business:
ftc.gov/video

Bureau of Consumer Protection
Business Center: business.ftc.gov

BCP Business Center:
Privacy and Data Security Resources

These resources & more can be accessed at: **business.ftc.gov**

Questions?

AUSTIN

BEIJING

BRUSSELS

DALLAS

DUBAI

HONG KONG

HOUSTON

LONDON

MOSCOW

NEW YORK

PALO ALTO

RIYADH

SAN FRANCISCO

WASHINGTON

bakerbotts.com

©Baker Botts L.L.P., 2019. Unauthorized use and/or duplication of this material without express and written permission from Baker Botts L.L.P. is strictly prohibited. Excerpts and links may be used, provided that full and clear credit is given with appropriate and specific direction to the original content.