PCI made easy for SMBs

10 February 2022

Loic Breat

Senior Manager, Regional Lead PCI EMEA

Payment Security Programs

verizon

Safe harbor statement

NOTE: In this presentation, we have made forward-looking statements. These statements are based on our estimates and assumptions and are subject to risks and uncertainties. Forward-looking statements include the information concerning our possible or assumed future results of operations. Forward-looking statements also include those preceded or followed by the words “anticipates,” “believes,” “estimates,” “expects,” “hopes” or similar expressions. For those statements, we claim the protection of the safe harbor for forward-looking statements contained in the Private Securities Litigation Reform Act of 1995. We undertake no obligation to revise or publicly release the results of any revision to these forward-looking statements, except as required by law. Given these risks and uncertainties, readers are cautioned not to place undue reliance on such forward-looking statements. The following important factors, along with those discussed in our filings with the Securities and Exchange Commission (the “SEC”), could affect future results and could cause those results to differ materially from those expressed in the forward-looking statements: adverse conditions in the U.S. and international economies; the effects of competition in the markets in which we operate; material changes in technology or technology substitution; disruption of our key suppliers’ provisioning of products or services; changes in the regulatory environment in which we operate, including any increase in restrictions on our ability to operate our networks; breaches of network or information technology security, natural disasters, terrorist attacks or acts of war or significant litigation and any resulting financial impact not covered by insurance; our high level of indebtedness; an adverse change in the ratings afforded our debt securities by nationally accredited ratings organizations or adverse conditions in the credit markets affecting the cost, including interest rates, and/or availability of further financing; material adverse changes in labor matters, including labor negotiations, and any resulting financial and/or operational impact; significant increases in benefit plan costs or lower investment returns on plan assets; changes in tax laws or treaties, or in their interpretation; changes in accounting assumptions that regulatory agencies, including the SEC, may require or that result from changes in the accounting rules or their application, which could result in an impact on earnings; the inability to implement our business strategies; and the inability to realize the expected benefits of strategic transactions.

As required by SEC rules, we have provided a reconciliation of the non-GAAP financial measures included in this presentation to the most directly comparable GAAP measures in materials on our website at www.verizon.com/about/investors

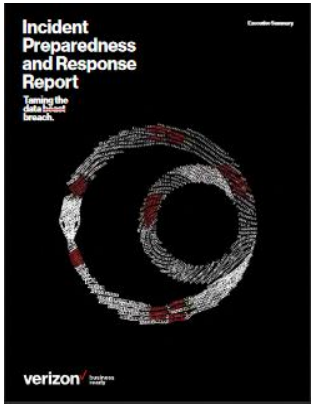
Welcome !

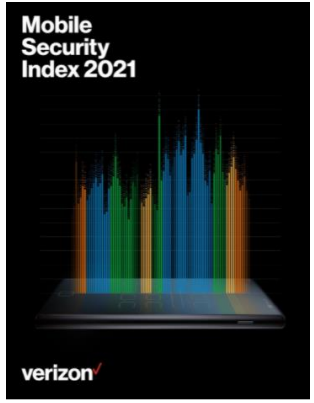
Loïc Breat
Senior Manager, Regional Lead PCI EMEA
Payment Security Programs

QSA since 2009
PCI 3DS QSA since 2020
CISA, CISM

+33 6 26 55 34 93
loic.breat@fr.verizon.com
https://www.linkedin.com/in/loicbreat/

Thought Leadership





20+
Years of Security Experience

60+
QSAs worldwide

600+
Security consultants in 30 countries

Smaller businesses are not immune to data breaches.

93%

Quoting the Verizon DBIR 2021, breaches continue to be mostly due to financially motivated actors (93%) in Small and Medium Business.

Top Patterns

System Intrusion, Miscellaneous Errors and Basic Web Application Attacks represent 80% of breaches

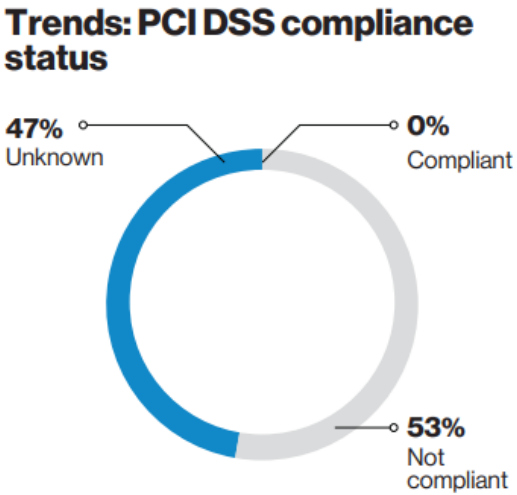
Source : Verizon 2021 Data Breach Investigations Report

44% of breaches involved credential data, followed by personal data, payment information, …

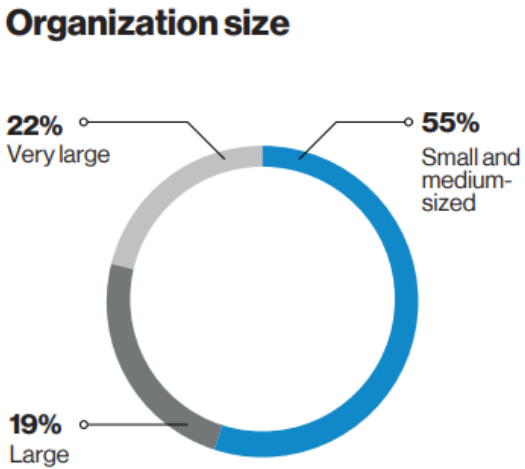
57% of breaches involved an External actor, 44% an Internal actor.

47% of SMBs find breaches within days or less.

Six-year data breach correlation trends



State of compliance at the time of the breach



Confirmed payment card data breaches by organization size

Dataset time span: 2014 to 2019

Source: Verizon 2020 Payment Security Report

Recommended data security items for SMBs

Recommended data security items for SMBs

Scope Reduction

- **Do not store any payment card data unnecessarily.**
- Do not capture credit card information in written form (unless the process is authorized and formally documented).

- Never store the magnetic track data from any card, in any format.
- **Never store the CID/CVV2 card security code in any format, in any way, ever .**

- **Choose a PCI-compliant payment gateway.**
- Use a PCI Security Standards Council (SSC)-validated point-to-point encryption (P2PE) solution

“If you don’t need it, don’t store it !”

Recommended data security items for SMBs

Secure Data

- **Use only secure transmission protocols**, such as Transport Layer Security (TLS) v1.2
- Make sure you only collect payment card information on a secure web page (originating from a PCI certified Service Provider).
- Secure and monitor the redirection to your Payment Service Provider.

Secure your data flows from end-to-end

Recommended data security items for SMBs

Secure Systems

- **Never use default passwords.**
- Set a strong password for your wireless router (if any)
- Make sure that all available security and encryption features are enabled and properly configured

- **Don’t host on the same server websites with different sensitivity levels.**

- Make an inventory and maintain hardware / software support for all critical system components.
- Be proactive in monitoring the support life cycle for all your critical system components.
- **Don’t forget to update your development frameworks too.**

Apply best practices always, everywhere !

Recommended data security items for SMBs

Security Monitoring and Testing

- Run **internal and external network vulnerability scans at least quarterly** and after any significant change
- Make sure that penetration test(s) are performed in adherence to PCI DSS Requirement 11.3
- Periodically **inspect device surfaces** to detect tampering
- **Regularly check terminals, PIN pads and computers** to ensure that rogue software or “skimming” devices are not installed

Monitor your components’ security on a regular basis

Recommended data security items for SMBs

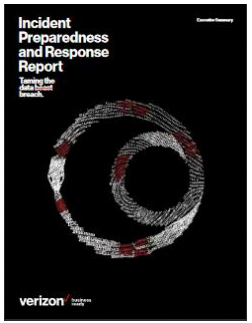
Incident Response

- **Implement basic incident response procedures**.
- Be prepared to respond immediately to a system breach.

- In the event of a breach or suspected data breach, **contact the acquiring bank immediately**

- **Provide appropriate training** to staff with security breach response responsibilities

Be prepared to respond to a breach



Recommended data security items for SMBs

Security Governance

- Create a security policy for your business that addresses all aspects of the PCI DSS

- **Educate your employees about security** and protecting payment data
- Ensure that staff is **educated on an annual basis** (at minimum) to include education on device tampering

- **Monitor service provider PCI compliance status to prevent lapses in compliance**

Don’t hide your security behind contracts. Be an actor of your compliance.

Real-world use cases

Real world examples - SMBs

Brick-and-mortar moving to E-Commerce

200 records breached

Prioritized Approach within 90 days + onsite PCI DSS assessment

Cost of breach > annual revenue.

Local sporting and event company

20k records breached

PFI engaged on Acquirer request with pressure from the Card Brand.

QSA engaged for compliance and audit.

Costs have been covered by a cyber insurance.

Key takeaways for SMBs !

- PCI is NOT your main activity. **Let a certified Service Provider** do the job for you.
- **Use** HTTP REDIRECT or IFRAME to integrate E-Commerce payment pages. **Use P2PE** payment terminals for face-to-face.
- Work actively with your(s) Service Provider(s) and **monitor their compliance** on a regular basis.
- **Partner with your Acquirer** and **proactively demonstrate compliance** through an SAQ.

Engage a QSA to:

- Help define, prioritize and support your compliance strategy.
- Validate your PCI scope and requirements applicability.
- Keep you on track along your compliance journey.

Remember, you are ultimately accountable for your PCI maintenance

Need to know more ? Contact us.
loic.breat@fr.verizon.com


verizon

Appendix

- 2021 Data Breach Investigation Report
- Verizon Incident Preparedness and Response (VIPR) Report
- Data Breach Digest 2018: Studies in cyber crime
- Mobile Security Index 2021
- 2020 Payment Security Report
- 2021 Payment Security Report Insights PCI DSS 4.0 whitepaper
- Overcoming PCI DSS compliance challenges for SMBs
- All our reports