

The image features a purple background with a wavy, tiger-stripe pattern. In the center, the letters "LSU" are displayed in a bold, yellow, sans-serif font.

LSU



Breaking In So You're Not Breaking Down

The Value of Penetration Testing

Presented by the LSU
Cyber Clinic Offense Team





So, let's break in.

- Target: a safe with valuable items inside.
- Our first task: get into the house.





We're in!

- How did we get in?
 - Key under doormat
 - Chimney
 - Unlocked back door
- What next?





On to the real hunt!

- It turns out our best bet is that it is in the master bedroom.
- Now, where is that safe?



LSU

There!

- But wait...is that a password pin-pad on it?





The final challenge:

- There's 10,000 possible combinations for this 4-character password- we'll never get the right one!
- Or will we...





Rolex time!

- We have secured the Rolex. Let's get out of here!



LSU

The Value of Testing:





Penetration Testing Steps:

- Preparation
- Reconnaissance
- Scanning
- Initial Access
- Lateral Movement
- Reporting



Reconnaissance and Scanning

- Without touching, what can you see?
- Interact, what do you find?
- Try everything!





Initial Access

- We brought our tools...
- We are inside, what now?
- Try everything!



Lateral Movement

- Were there issues with moving between rooms?
- Where is the critical material?
- Try... everything!





The Last Step...

- Passwords make or break!
- Is there a policy? Account lockout?
- Try... You get it by now.





Time to Report!

- Goal achieved, now what?
- Our report should cover all the bases to prevent all attacks.



LSU

A Common Pitfall...

They will never
break in!





The Problem

- Social Engineering
- Phishing
- Assumed Breach



LSU

Demo!!!



<https://youtu.be/q2sTln1M380>

LSU

Who is This?



LSU

Who is This?



MAERSK



LSU

Who is This?



MAERSK



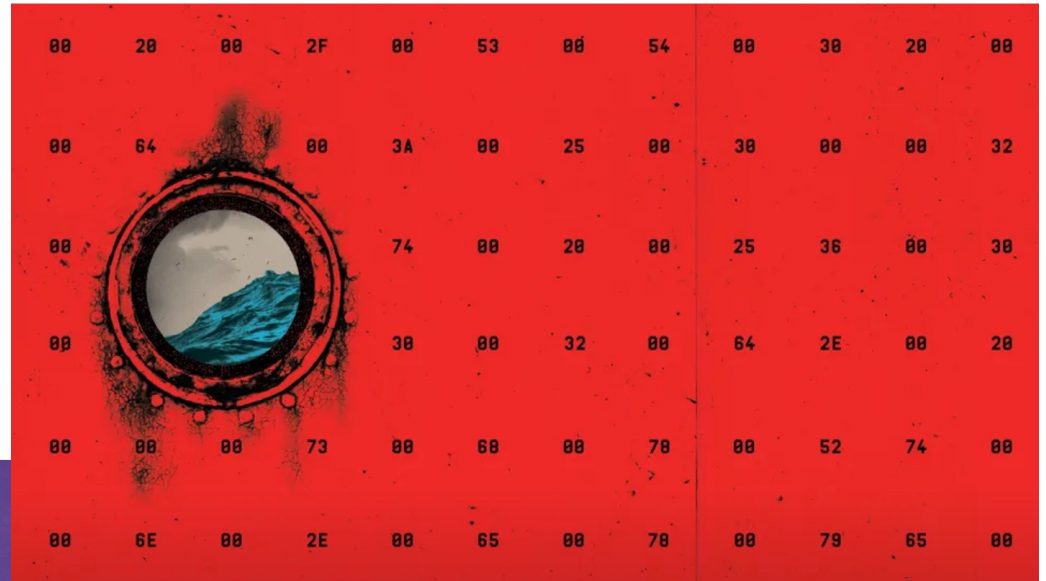
WIRED

BACKCHANNEL BUSINESS CULTURE GEAR MORE ▾

SUBSCRIBE

The Untold Story of NotPetya, the Most Devastating Cyberattack in History

Crippled ports. Paralyzed corporations. Frozen government agencies.
How a single piece of code crashed the world.



MIKE MCQUADE

LSU

Who is This?



MAERSK

WIRED

BACKCHANNEL BUSINESS CULTURE GEAR MORE ▾

SUBSCRIBE

The Untold Story of NotPetya, the Most Devastating Cyberattack in History

Crippled ports. Paralyzed corporations. Frozen government agencies. How a single piece of code crashed the world.

The damage caused by NotPetya has been pegged at more than \$10 billion. Maersk alone lost \$250 million and \$300 million. Other companies affected included Mondelez, Merck, WPP,

Reckitt Benckiser, Saint-Gobain and TNT Express.

MIKE MCQUADE

LSU

Who is This?



LSU



Who is This?
Welltok®



LSU

Who is This?

Welltok®



Welltok
Welltok drives consumer actions that matter.
Wellness and Fitness Services · Denver, CO · 27K followers · 201-500 employees

[+ Follow](#) [Visit website](#) [...](#)

Who is This? Welltok®

Welltok data breach exposes data of 8.5 million US patients

By **Bill Toulas**

November 22, 2023 01:22 PM 0



Healthcare SaaS provider Welltok is warning that a data breach exposed the personal data of nearly 8.5 million patients in the U.S. after a file transfer program used by the company was hacked in a data theft attack.

Who is This?

Welltok®

Welltok data breach exposes data of 8.5 million US patients

By **Bill Toulas**

November 22, 2023 01:22 PM 0

Info Leaked Includes

- Full names,
 - email addresses,
 - physical addresses, and
 - telephone numbers.
- For some, it also includes
- Social Security Numbers (SSNs),
 - Medicare/Medicaid ID numbers, and
 - certain Health Insurance information.

Healthcare SaaS provider Welltok is warning that a data breach exposed the personal data of nearly 8.5 million patients in the U.S. after a file transfer program used by the company was hacked in a data theft attack.



Who is This?
Welltok®

IMPACTED INSTITUTIONS

The impact of the breach impacted institutions in various states, including Minnesota, Alabama, Kansas, North Carolina, Michigan, Nebraska, Illinois, and Massachusetts, with the following healthcare providers said to be impacted:

- Blue Cross and Blue Shield of Minnesota and Blue Plus
- Blue Cross and Blue Shield of Alabama
- Blue Cross and Blue Shield of Kansas
- Blue Cross and Blue Shield of North Carolina
- Corewell Health
- Faith Regional Health Services
- Hospital & Medical Foundation of Paris, Inc. dba Horizon Health
- Mass General Brigham Health Plan
- Priority Health
- St. Bernards Healthcare
- Sutter Health
- Trane Technologies Company LLC and/or group health plans sponsored by Trane Technologies Company LLC or Trane U.S. Inc.
- The group health plans of Stanford Health Care, of Stanford Health Care, Lucile Packard Children's Hospital Stanford, Stanford Health Care Tri-Valley, Stanford Medicine Partners, and Packard Children's Health Alliance
- The Guthrie Clinic

Who is This?

Welltok®

Welltok.

Welltok

Welltok drives consumer actions that matter.

Wellness and Fitness Services · Denver, CO · 27K followers · 201-500 employees

+ Follow

Visit website



Now Hiring

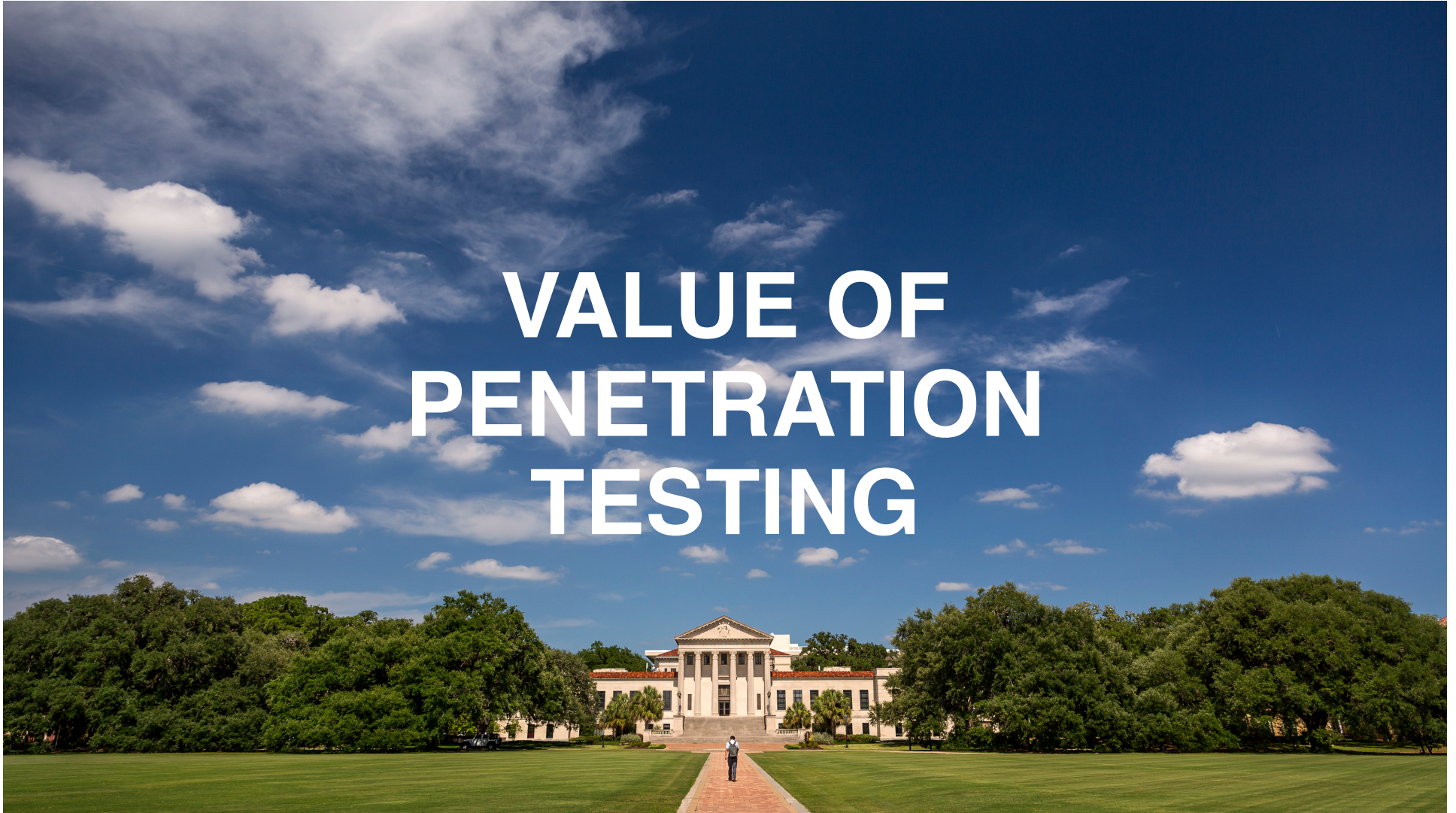
BlueCross BlueShield of South Carolina is an independent licensee of the Blue Cross Blue Shield Association.

BlueCross BlueShield of South Carolina

South Carolina's largest and oldest health insurance company

Insurance · Columbia, South Carolina · 34K followers · 10K+ employees

VALUE OF PENETRATION TESTING



LSU

Questions?

