Social Engineering: Tales from a Non-Traditional IT Audit

Kimberly Hagara, Vice President, Audit Services
UTMB Health

Paul Douglas, Associate Consulting Director
P&N

Agenda

1. The Risk: What is Social Engineering
2. The Project: UTMB Health's Story
3. The Controls: Internal Audit Considerations
4. The Trusted Advisor: Internal Audit and Cybersecurity

P&N Postlethwaite & Netterville

utmb Health

The Risk

P&N
Postlethwaite & Netterville

utmb Health

What is Social Engineering?

- Phishing and Spear Phishing

- Vishing and SMS texting

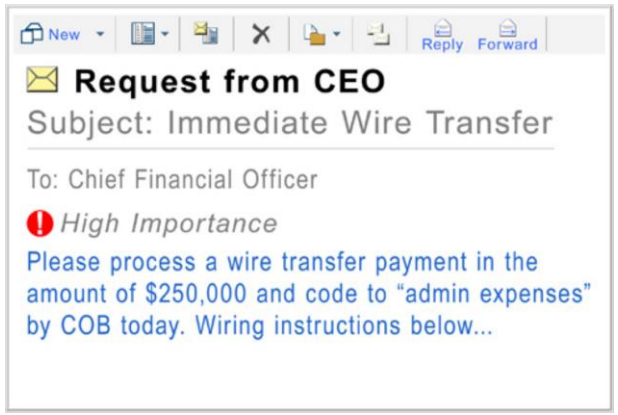
- Baiting and Physical Exploits

P&N Postlethwaite & Netterville

utmb Health

What Could Go Wrong?

- Employee W2 extracts – Seasonal exploit

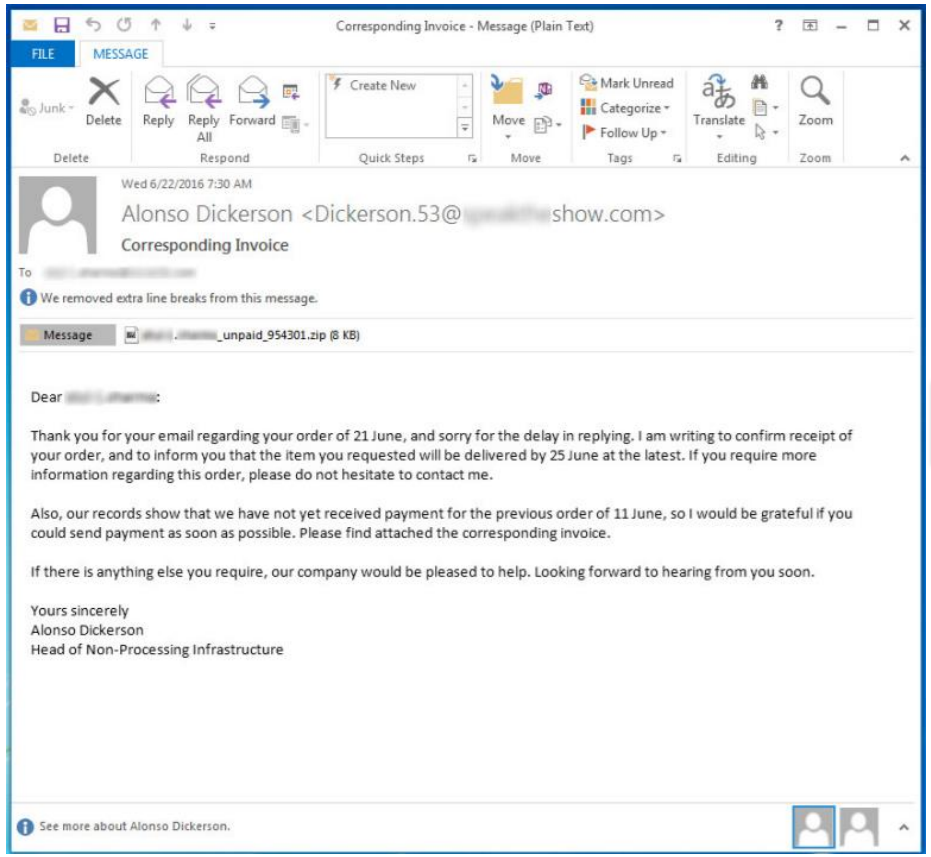


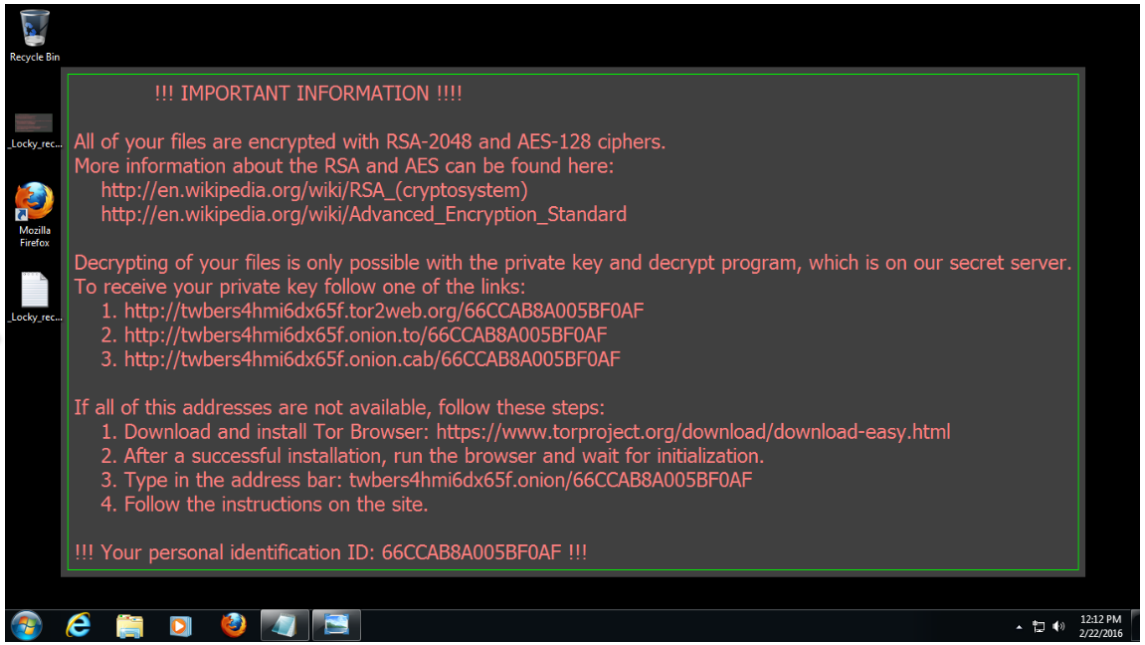
- Wire fraud schemes – Executive exploit

P&N Postlethwaite & Netterville

utmb Health

What Could Go Wrong?

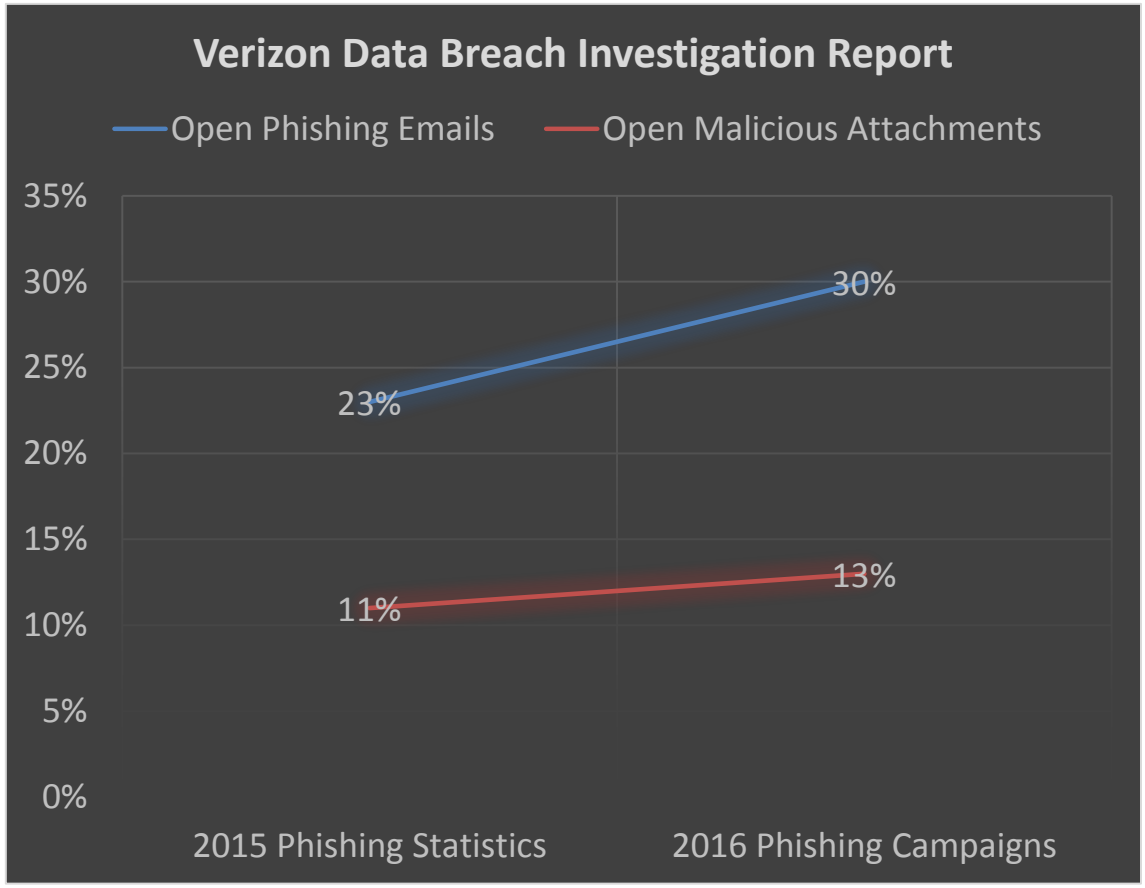




P&N
Postlethwaite & Netterville

utmb Health

Data Behind the Risk



- 89% of phishing attacks originate from organized crime syndicates (source: Verizon).
- 95% of all attacks on enterprise networks are the result of spear phishing (source: SANS Institute).
- Phishing will remain the primary method attack delivery through the year 2020 (source: Gartner)

P&N Postlethwaite & Netterville

utmb Health

Inherent Risk Exposure?

Target	Level of Susceptibility?
▪ New Employee	?
▪ Contractor	?
▪ Executive and Administrative Assistants	?
▪ C-Suite	?
▪ HR	?
▪ Legal	?
▪ Security Personnel	?
▪ IT Personnel	?
▪ Finance and Accounting	?
▪ Marketing/Communications	?

Risk Scenarios – Threat/Non-Threat?

Social Engineering Technique	Risk Scenario	Risk Exposure*	Level of Effort by Cyber-Criminal
Phishing	Opening a malicious email?	Very Low	Very Low
Phishing	Clicking a malicious link?	Low	Very Low
Phishing / Baiting	Opening a malicious file?	Medium	Very Low
Baiting	Inserting a malicious USB drive?	Medium	Medium
Phishing / Baiting	Running program / executable?	Very High	Very Low
Phishing / Baiting	Running a macro in a malicious file?	Very High	Very Low
Phishing / Baiting / Vishing	User credential theft?	Very High	Very Low
In-Person Exploit	Theft of IT Assets, Sensitive Data	Very High	Medium – Very High

*assumes a moderate level of security and system hardening is in place.

P&N Postlethwaite & Netterville

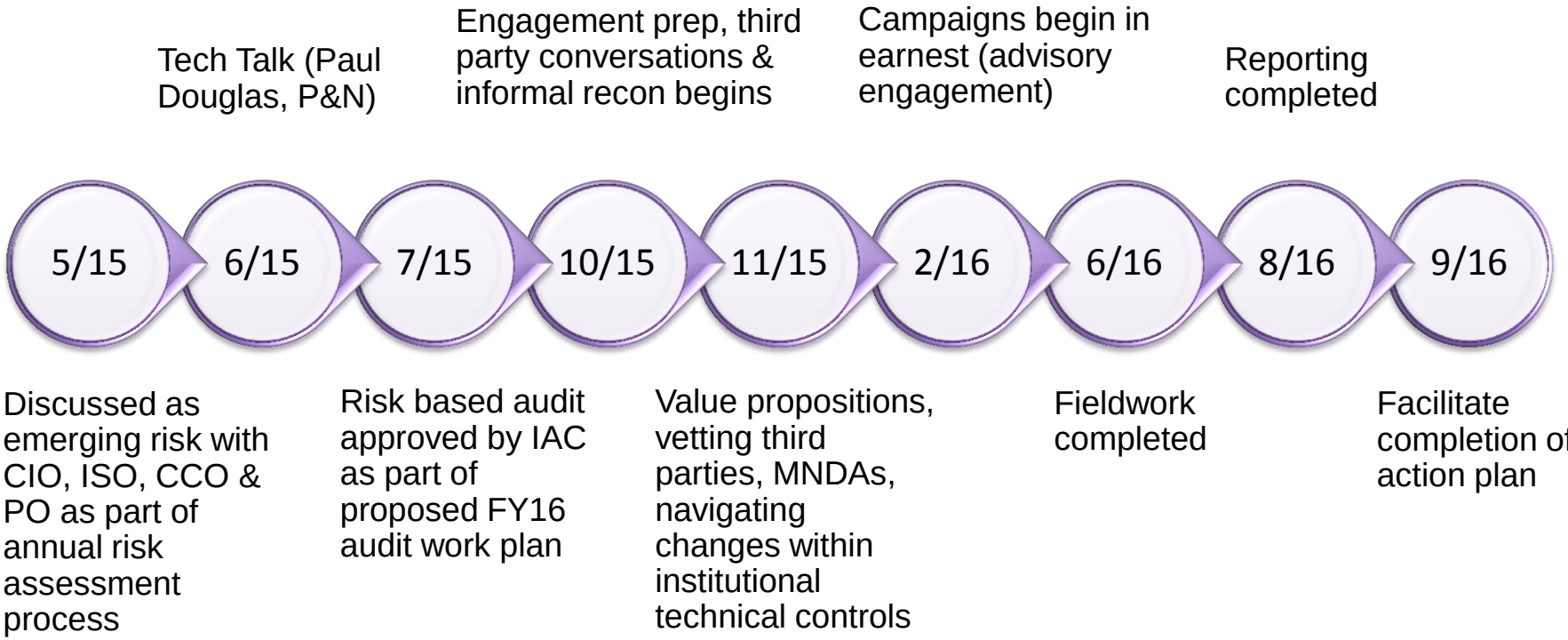
utmb Health

The Project

P&N
Postlethwaite & Netterville

utmb Health

Engagement Timeline



Engagement Premise

- Assess the ease of gaining access to buildings, infrastructure, automated information systems, or confidential/sensitive data through methods primarily relying upon human interaction, persuasion or deception (i.e., “a sense of susceptibility, or vulnerability”).
- Replicate real world scenarios (both internal and external threats) with varied levels of sophistication and without any notification of testing activities.
- Take reasonable care to do no harm.
- Educational, non-punitive, anecdotal findings.
- Facilitate development of action plan for sustained improvement.
- …and ultimately get a feel for what it might mean to “operationalize” this type of testing.

Engagement Protocol

- Attorney-Client and attorney work-product privileges.
- Adaptive and opportunistic exploitation.
- All active engagement participants sign non-disclosure agreements.
- IT Audit Manager (or designee) will be notified prior to third parties initiating any potentially invasive campaigns.
- University Police will be notified prior to any physical testing or walkthroughs performed during off-hours.
- Suspected or actual compromised data and/or physical devices will be placed within the protective care of the Privacy Officer.
- University Police will be notified of any physical asset removed from its original location and placed within protective care of the Privacy Officer.
- Any change/compromise in the physical/logical state of an IT asset (not-removed) will be communicated to the Chief Information Officer.
- Any egregious violation of applicable governance will be brought to the immediate attention of Senior VP/General Counsel.
- Provide regular status to Senior VP/General Counsel.

Engagement Stakeholders

Tone from the Top

- Senior VP & General Counsel (sponsor)
- VP & Chief Compliance Officer (owner)
- VP, Legal Affairs
- Police Chief, Assistant Chief, Lt. (Operations/Patrol)
- CAE
- CIO
- ISO
- PIO

From the Bottom Up

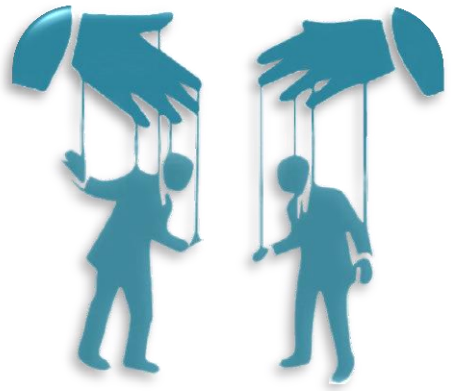
- IT Audit Manager (engagement lead)
- IT Auditor (chauffer)
- Privacy Officer (guard rails)
- Web Developers (2)
- Advocate from the trenches
- Helpdesk tickets
- Exchange Engineer
- Advocate from the trenches
- Hall monitor
- Police Technical Manager

Engagement Tactics

- 40+ buildings, 100+ walkabouts
- 150+ baits
- Multiple campus/satellite locations; offices, closets, PCs
- Phishing (e.g., password stringency test, inbox notifications)
- Spear Phishing (e.g., April Fool's Day)
- Vishing (e.g., IT maintenance impersonation)

Engagement Methods

- Assumed identities (persons, domains, websites)
- Reconnaissance (“wandering” the campus)
- Door shimming/bumping & weak passcodes
- Facility intrusion (exterior piggybacking)
- Building walkthroughs (interior penetrations)
- Desktop hacking (“targets of opportunity”)
- Data exfiltration (unsecured login sessions)
- OCD tests
- Police encounters
- Baiting
- Pharming (aggressive bait placement)
- Security camera/records retention testing
- “Snatch and Grab”
- Lost & Found procedures
- Dumpster diving
- On-site impersonations
- Phone impersonations
- Password shares



- Visitor/Guest management
- Signature spoofs
- Spoofed domain names & websites
- Data mining (OSINT - publically available)
- Data leakage (PIAs, Intranet)
- Application/User authentication testing
- Vulnerability scans/tests
- Technology patching/configuration testing
- Ransomware susceptibility
- Executive calendar accessibility
- Incident response notifications
- Phishing (enticements)
- Spear phishing (emotional triggers)
- Pretexting (contextual information)
- Vishing (phone version of phishing)
- Whaling (Executive Management)
- Litmus testing (“give me your best shot”)
- Cat Phishing (PG13)

P&N Postlethwaite & Netterville

utmb Health

Engagement Takeaways

- Internal Audit's relationship with Executive Management says a great deal about your culture.
- At the end of the day layered security defenses are porous and ultimately your employees become your perimeter!
- Employees can be your greatest vulnerability or your best defense against social engineering attacks.
- Everything worthwhile is uphill!

Structuring your Team

- Right balance of internal and external resources.

The Controls

P&N
Postlethwaite & Netterville

utmb Health

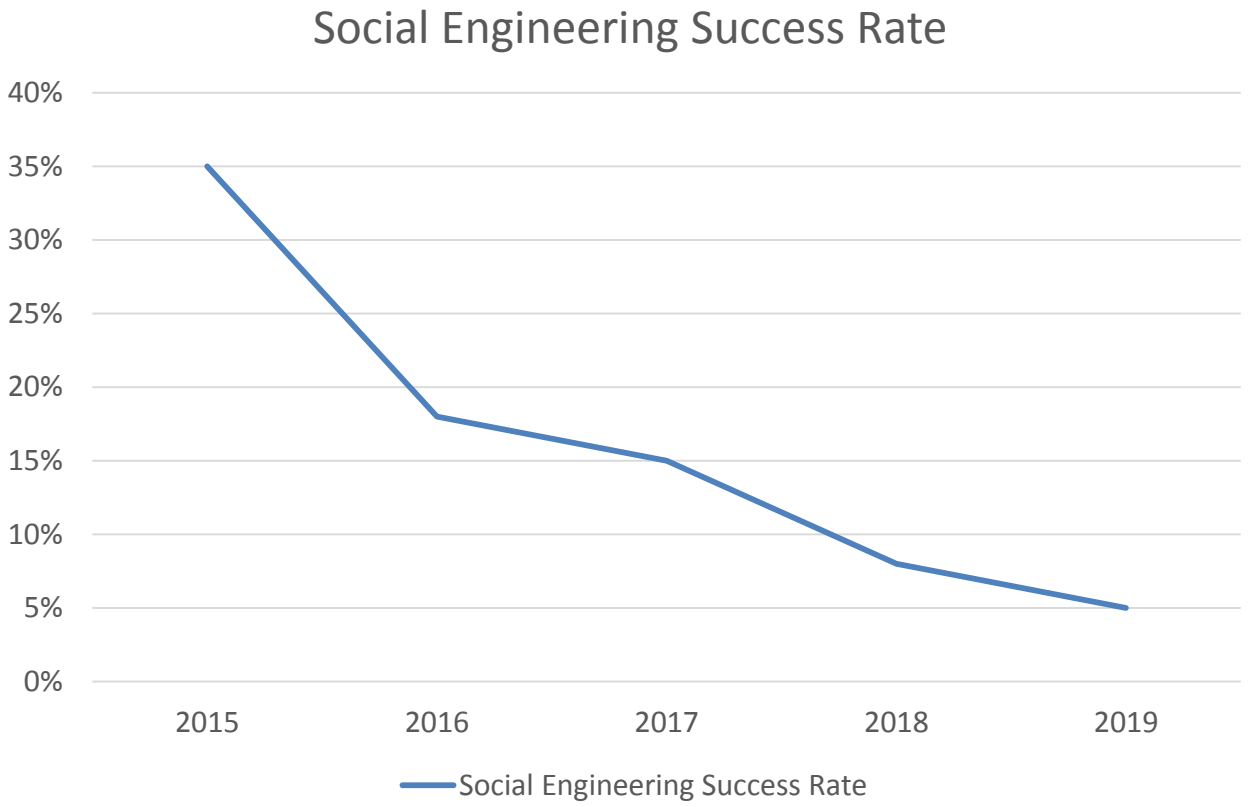
It's more than just phishing…

- Lost and found procedures
- Incident response procedures
- Building entrances
- Building interiors (restricted/secured space)
- Extent of police presence & camera coverage
- Hardcopy (disposal to destruction)
- Desktop configurations (are controls what you expected)
- Non-sanctioned software use
- Vulnerability scans (end user devices)
- Extent of encryption
- Publically displayed login credentials

Related NIST 800-53 Controls

- AT-01 SECURITY AWARENESS AND TRAINING
- IR-01 INCIDENT RESPONSE POLICY AND PROCEDURES
- SC-39 PROCESS ISOLATION
- SC-41 PORT AND I/O DEVICE ACCESS
- SC-44 DETONATION CHAMBERS
- MP-07 MEDIA USE | PROHIBIT USE WITHOUT OWNER
- IA-4 PROHIBIT ACCOUNT IDENTIFIERS AS PUBLIC IDENTIFIERS
- SI-8 SPAM PROTECTION
- SC-7 PREVENT UNAUTHORIZED EXFILTRATION
- AC-19 FULL DEVICE / CONTAINER-BASED ENCRYPTION
- SC-28 PROTECTION OF INFORMATION AT REST

Measuring the Effectiveness of Training



The Trusted Advisor

P&N
Postlethwaite & Netterville

utmb Health

Adding Value

- As risks continue to evolve, so too must the internal audit function.
- Progressive approaches; different conversations and levels of services.
- Help drive organizational change; reducing the exposure to social engineering threats.
- Provide insights and recommendations on an important risk matter.

The Case for Internal Audit & Cybersecurity

Independent and Objective	⇨	**Higher Degree of Confidence**
Risk Focused	⇨	**Stronger Mitigation Plan**
Control and Operating Effectiveness	⇨	**Cybersecurity is Not Just a Point in Time!**

P&N Postlethwaite & Netterville

utmb Health

Closing Thoughts

P&N
Postlethwaite & Netterville

utmb Health