EMERGENT
NETWORK DEFENSE

Use Case:

The Real Vulnerability of the 2017 Equifax Breach

What Happened?

The technical cause of the 2017 Equifax data breach has been traced to a known flaw in the Apache Struts open web application framework. The actual *business vulnerability* that led to the breach goes much deeper.

> **What was clearly lacking was executive risk clarity, combined with a weak risk management culture.**

The Equifax risk culture was apparent when former CEO Richard Smith testified before Congress about the breach. While he took *responsibility* as the chief executive, he placed *culpability* onto a single IT technician for failing to install the patch. A forward-leaning organization with fully-engaged executives would have had more robust visibility into and governance over the myriad digital risk exposures in the organization. Business decisions would have been made in light of real-time risk intelligence, and the top executive team would have been more engaged.

Visibility and Action Gaps

1. **Lack of executive engagement and clarity into risk exposures** – Smith was not briefed for 18 days after the breach was discovered and didn't notify the board for another five days.
2. **Executives' inability to prioritize digital risks** – Smith never asked whether a PII leak was a possibility and only reviewed security posture quarterly.
3. **Failure to align risk management with business interests** – Equifax was slow to implement a known fix, suggesting that there was no urgency identified by business stakeholders to protect their data.

By taking the time and focus to think through digital impacts, connect them to real-life scenarios, and instrument scenario exposure using pre-existing data, Equifax could have easily flagged the known Struts flaw and prioritized the fix, saving billions of dollars and several top executives' jobs.

Emergent's Digital Risk Management Solution

1. The Emergent Instinct Engine **cuts through stove-piped, tactical data** to provide executives with real-time clarity to **understand their digital exposure to business losses**.
2. Swarming artificial intelligence continually **assesses thousands of risk scenarios**, ranking them by their **exposure** and potential **impact**.
3. Business Unit reporting **gives business and non-technical personnel** a view of how *their operations* are exposed to digital risks, **empowering them to understand and act** on out-of-balance risk-taking.

About the Instinct Engine

The Instinct Engine is an on-premises or cloud-based software platform for discovering, quantifying, and communicating an organization's digital risks. It answers three basic questions:

- ***Where* is our *next* digital incident?**
- ***How bad* could it be and *is it too much*?**
- ***What should we do* about it?**

The platform uses a broad catalog of **real-life and machine-generated exposure scenarios** to discover hidden digital risks. **Lightweight data integration** connectors to over 40 pre-built data sources mean it can be installed in a week and instrumented to existing enterprise data sources. Swarming AI algorithms quickly **discover and visualize emerging risk areas so you can "see around the corner" and act before the consequences occur**.

To schedule a demo, visit http://endsecurity.com or email seetheswarm@endsecurity.com

1133 15th Street NW, 12th Floor, Washington, DC 20005