Your Data:
Protect its Integrity

Connectivity and smallness

The growth in the absolute amount of data can be attributed to several transformative technologies. The developed or post-industrial economies have largely changed to service or information economies created by connectivity. This new "smallness" necessitates even more connectivity to keep everything functioning. The web afforded us the ability to connect, communicate, work, research, surf and stream media at anytime and anywhere with astonishing speed. The advent of portable devices; i.e. laptops, smartphones, and tablets permits us the opportunity to work from wherever we choose. The reality is that we are tethered, more than ever, to our devices and our jobs. It is this connection to our jobs that creates great promise and opportunities while at the same time greater enterprise exposure and risk. ***More than ever, there are multitudes of entrances into an organization, its systems, and arguably one of its most valued assets: data.***

Your enterprise is more vulnerable than ever

We access our work through the front door each day and systems at our desks thru workstations and laptops. When you turn the lights off, set the alarm and leave your office, your door is still open. That open door is who accesses your systems and information whether it be via the laptop, smartphone and tablet. It's as if the door is never closed. Firewalls and other detection devices are not faultless. Social engineering attacks such as malware, ransomware, sphere-phishing and malicious code insertions are just a click away from permeating your systems and data. And, it's not just the outsiders that are of concern; enterprises must also concern themselves with malicious insiders, exploited insiders and careless insiders. *"No locale, no industry or organization is bulletproof when it comes to the compromise of data." Those words from Verizon's "2016 Data Breach Investigations Report" neatly summarized the cyberthreat environment today. There is no immunity. This year's wave of cybercrime statistics suggest that threats are well-funded, increasingly nefarious and more costly to victimized organizations. In fact, IBM President and CEO Ginni Rometty described cybercrime as "the greatest threat to every profession, every industry, every company in the world."*

How attacks are classified

Per Verizon's 2016 Data Breach Report, there are many methods by which bad actors can hack an organizations' systems. Clearly, there is an ebb and flow for each category as enterprises recognize, get smarter and adapt to addressing each type of potential attack. Interestingly, the major categories never go away; they temporarily go out of favor until the hackers re-group and adapt to the new defenses. They are relentless.

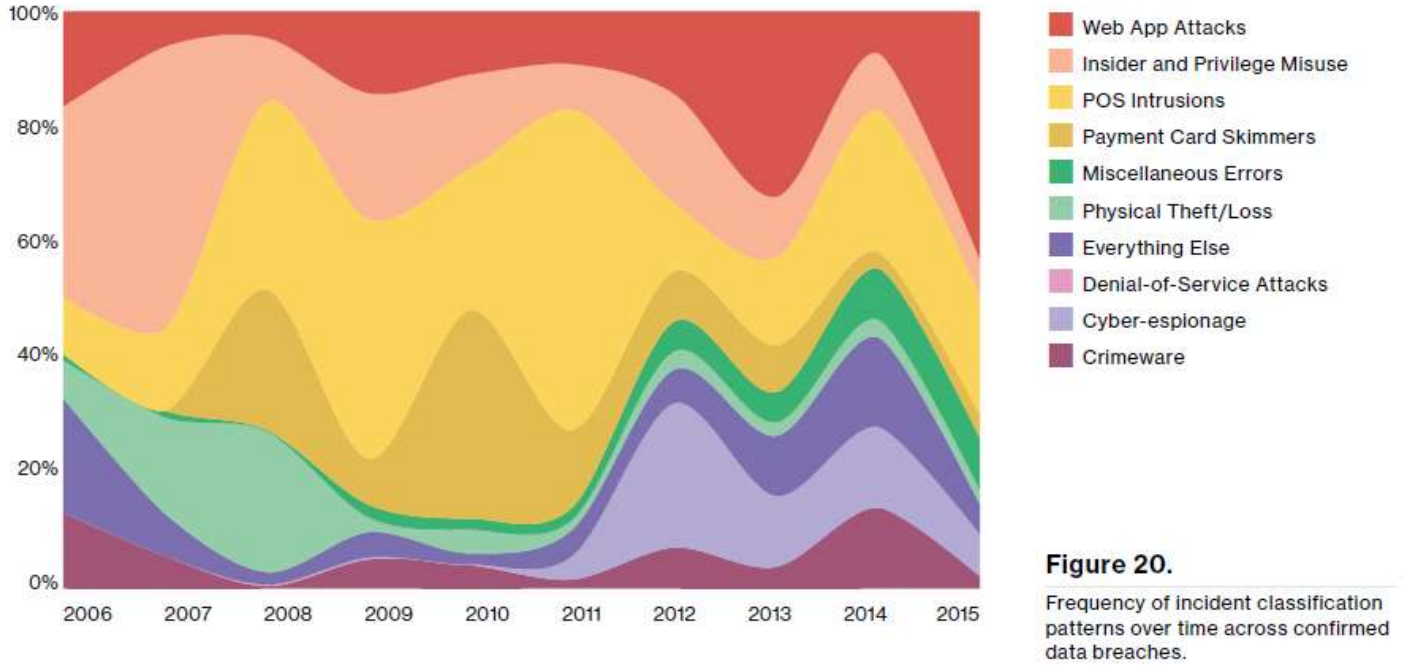

Figure 20.
Frequency of incident classification patterns over time across confirmed data breaches.

Source: Verizon 2016 Data Breach Report

At the end of the day, nefarious actors will never stop their attempts to infiltrate your organization; no one is immune from a potential attack. ***There are ominous adages that are quite commonly referred to when categorizing cyber-attacks: there are two types of companies; those that have been hacked and those that will be hacked, or alternatively, those that have been hacked and those that do not know that they have been hacked.*** And once compromised, how does an organization make the determination concerning the integrity of its data, report on and restore what has been stolen and determine what has been manipulated or corrupted? ***This is why a comprehensive strategy focused on data integrity is essential.***

Data Realities

- Data is as asset
- Data integrity is critical
- Data growth is exponential

Security Realities

- Information is under attack
- Your brand is bound to your data security
- Access points are proliferating – internal and external
- Security will always be a concern – physical and virtual

Security Considerations

- Many organizations fail to have or fail to execute on their security strategy
- The effectiveness of a contingency plan is commonly not known until it is needed
- Many organizations fail to recognize malicious, careless and exploited insiders
- Approx. 30% of malicious emails get opened despite increased training and awareness
- Firewalls, screening and detection systems are not flawless – layered approach is crucial
- Outsourcing and third party service providers present security challenges
- Disparate data locations present unique challenges and vulnerabilities
- Following a breach, proof of tampering, theft and corruption is a challenge
- Audit logs are under attack by hackers to cover their tracks & hide what they have done
- Compliance is a growth industry: expect more regulation and stricter enforcement
- Understand your retention and encryption requirements

Data and Storage Considerations

- All storage solutions are not created equal: security, access visibility and transparency
- Exclusive on-premise storage increases risk: mix of on-premise, cloud or hybrid?
- Accessibility and integrity of stored data is frequently overlooked until it’s needed

What is ULedger Data Assurance?

Uledger Data Assurance provides a platform that provides document level content verification, immutable audit trail coupled with identity authentication. This allows for certainty in data creation and subsequent activity.

Uledger has developed proprietary Blockchain solutions that enables our clients to create a permanent and independent 3rd-party record of any type of data, whether it's an electronic medical record, image, contract, journal entry, email or any other type of data. Our audit trail solution logs the creation of data and the activity of that data going forward. Our Blockchain approach creates indisputable proof of the evolution of data to information and finally to fact.

ULedger offers our Blockchain Data Assurance audit logs for both companies that choose to archive and maintain control of their data and for those who take advantage of our distributed archival solution. In both scenarios, the audit trail is independent, corroborated by multiple nodes, and provides a record of a "fact" at any point in time, ensuring that history cannot be re-written.

In true Blockchain fashion, each transaction that Uledger logs is time-stamped and hashed by multiple independent parties to corroborate the event and the truth of the event, while only you have access to the underlying data.

Uledger leverages a combination of technologies, including:

- Permissioned Blockchain
- Cryptography
- Merkelization
- PKI
- SKI
- Google Roughtime

Uledger technology allows for a for a highly scalable solution that can handle signing and tracking of virtually any discrete data element. Our open API standards make it Integratable with existing infrastructures. Out technology acts as an additional layer of verification and integrity on top of an existing security environment.

Product Overview and Capabilities

Uledger Data Assurance can be used in a stand-alone manner or in combination with other security layers. Key capabilities include:

- Incorporate Blockchain hash and time-stamps on document content
- Store audit trail within document, creating permanent and discreet record of:
  - ✓ Content
  - ✓ Changes
  - ✓ History
- Archive resulting document locally or to ULedger servers
- Optionally store document locally and audit trail externally for redundancy
- Identify and report on any attempted changes to signed data

ULedger Boise
910 Main Street, Suite 252
Boise, ID 83702

ULedger Kosovo
Ali Kelmendi 26/1
Prishtina 10000 Kosovo

ULedger Chicago
190 S. LaSalle Street, Suite 450
Chicago, IL 60603