CONGRESO DE
PREVENCIÓN
DEL
FRAUDE Y
SEGURIDAD

Construyendo **experiencias** desde un **entorno seguro.** ◀◀◀

FECHA
15 - 16
DE NOVIEMBRE /2018
HOTEL GRAND HYATT BOGOTÁ

Ricardo Bueno

Next Generation Data Protection

The network is **responsible** for protecting your data...

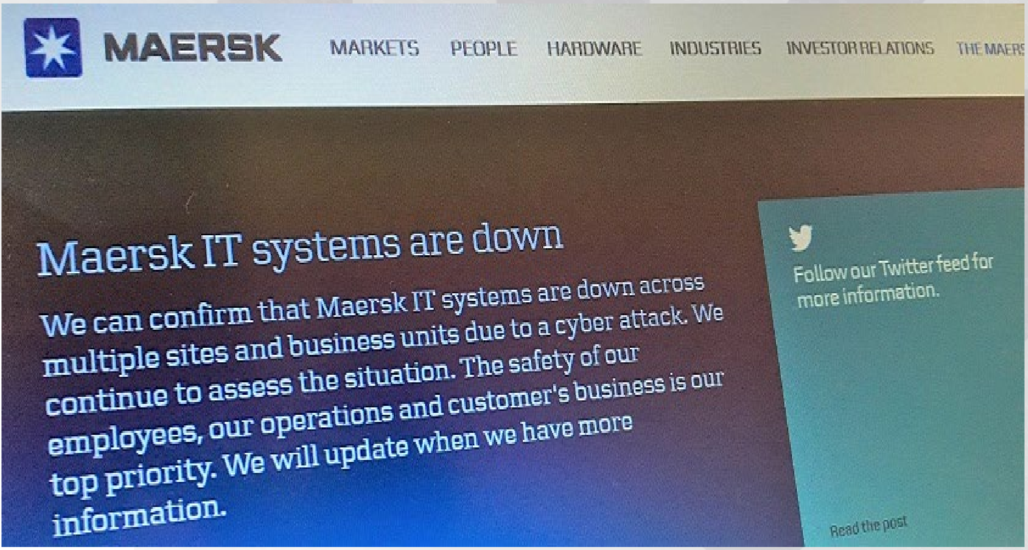
...and its not working

Maersk Ransomware Attack

Reinstall 4,000 servers

Reinstall 45,000 PCs

Cost: $300M



Maersk IT systems are down

We can confirm that Maersk IT systems are down across multiple sites and business units due to a cyber attack. We continue to assess the situation. The safety of our employees, our operations and customer's business is our top priority. We will update when we have more information.

Follow our Twitter feed for more information.

Read the post

A simple click of a nefarious email **collapsed** the entire cyber security infrastructure.

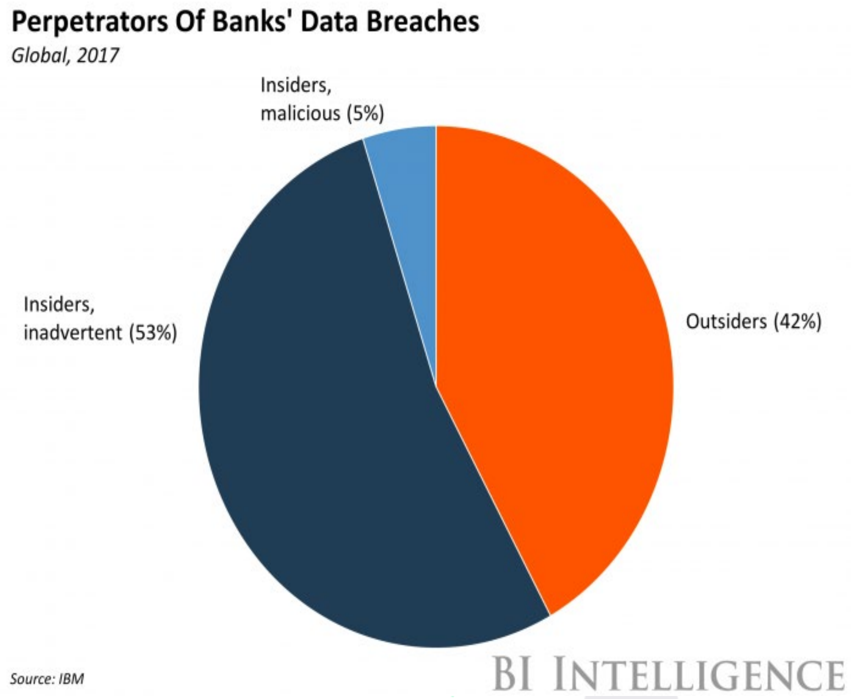
Insider Bank Breaches

Data breaches are on the rise in financial services (FS): 200 million financial services records were breached throughout 2016, accounting for a 937% year-over-year rise.

- FS was the most-attacked industry out of those examined in 2016 — these firms were breached 65% more than the average organization in all other industries in the study.

- Cyber criminals are waking up to the extent of banks' lax security faster than the institutions themselves.

- Establishing an independent data protection capability that prevents insider threat actions will dramatically decrease data breach events.



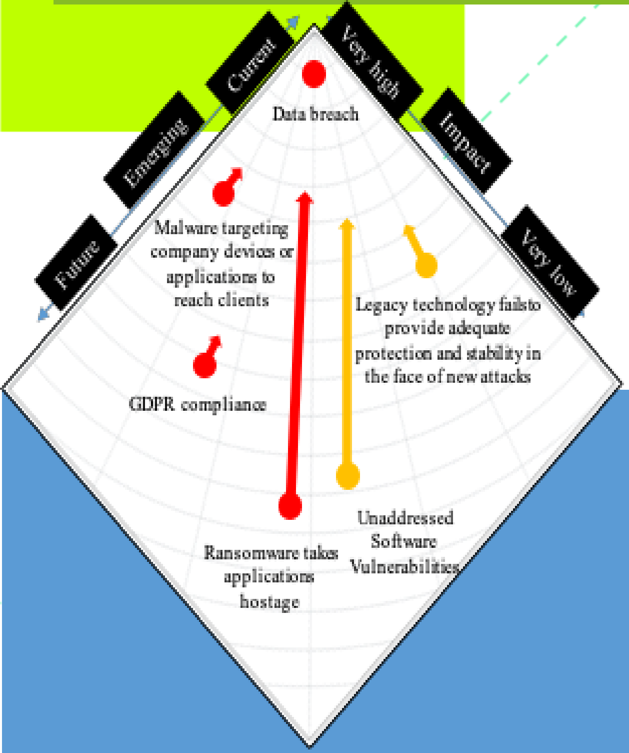
Perpetrators Of Banks' Data Breaches

Global, 2017

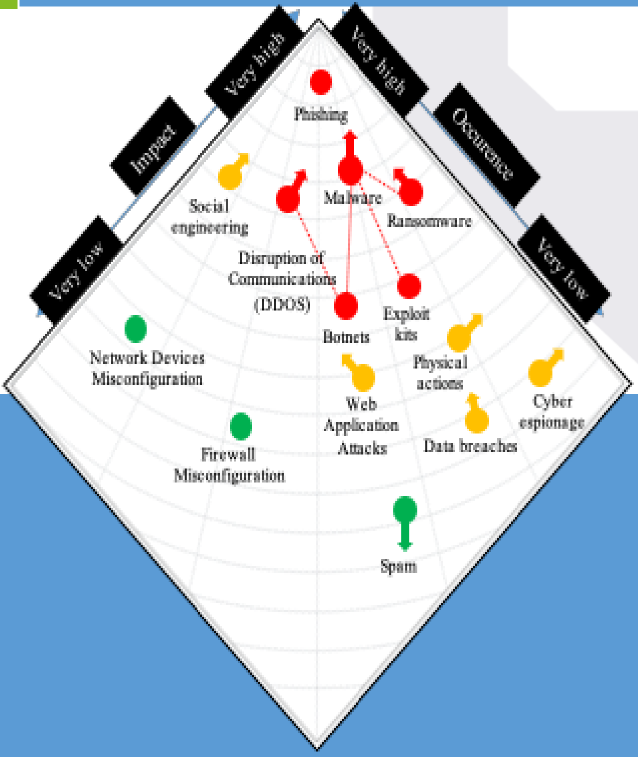
Source: IBM

Threat Perspectives

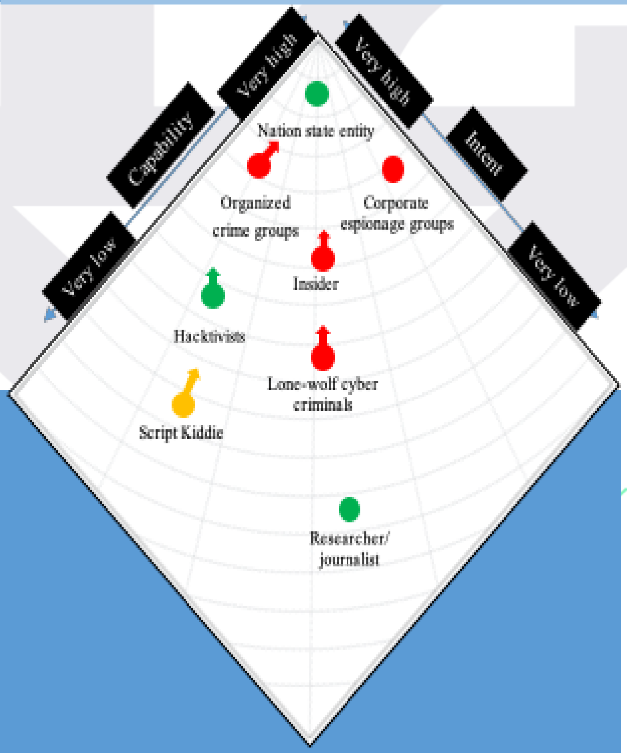
TOP THREAT SCENARIOS


Current
Emerging
Future
Very high
Impact
Very low
Data breach
Malware targeting company devices or applications to reach clients
Legacy technology failsto provide adequate protection and stability in the face of new attacks
GDPR compliance
Ransomware takes applications hostage
Unaddressed Software Vulnerabilities

TOP ATTACK VECTORS



TOP ADVERSARY GROUPS



NOTABLE CYBER SECURITY EVENTS

- Legacy technology is susceptible to attack.
- Ransomware disrupts businesses globally.
- Unaddressed software vulnerabilities can weaken defences.

KEY TAKEAWAYS

Threat actors develop capabilities and change their attack vectors to take the least difficult approach into your company. For this sector we observed high profile actors targeting for monetary gain, while hacktivism focused on disruption. Tracking industry trends can assist in understanding attack vector changes and form protective mitigation strategies.

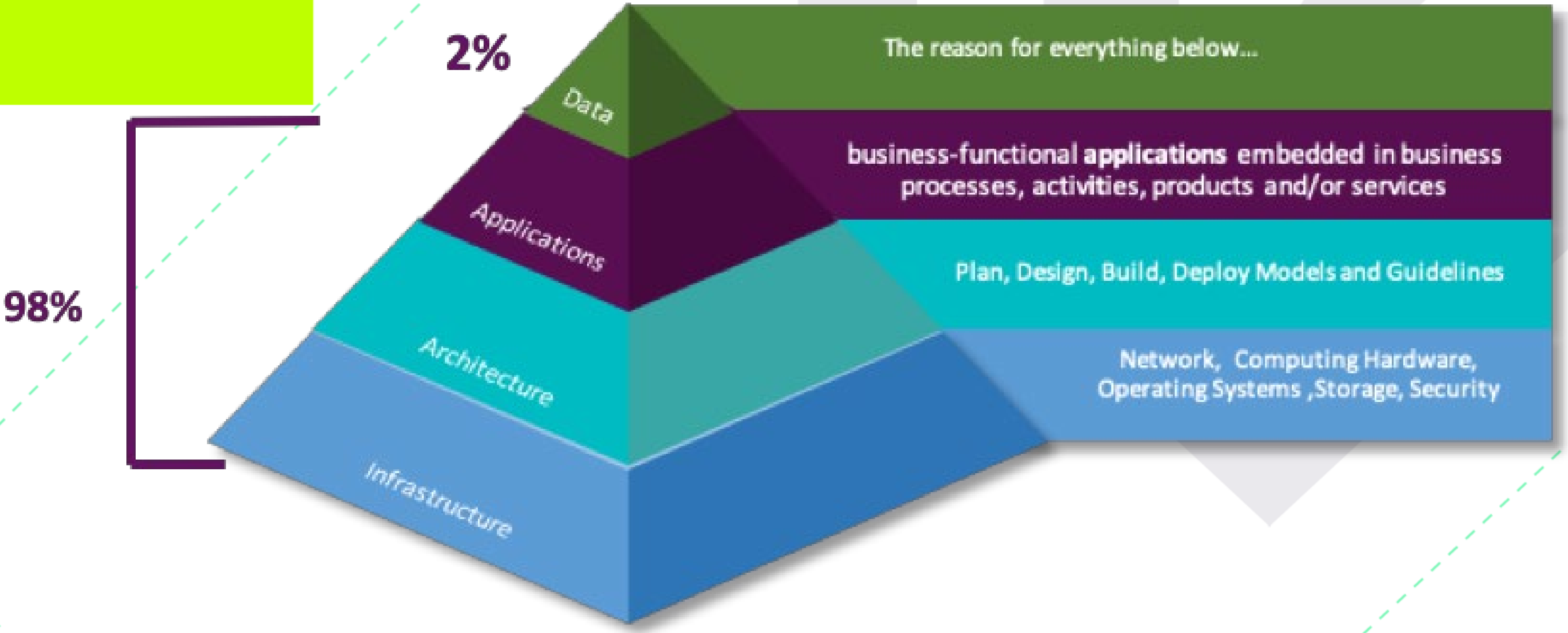
Zero Trust Network Paradigm

The Zero Trust Network paradigm relies on a core principle of ”Never Trust, Always Verify”.

- The network is always assumed to be hostile.
- External and internal threats exist on the network at all times.
- Network locality is not sufficient for deciding trust in a network.
- Every device, user, and network flow is authenticated and authorized.
- Policies must be dynamic and calculated from as many sources of data as possible.

But there is something still missing…

The Enterprise IT Stack



The reason for everything below...

business-functional **applications** embedded in business processes, activities, products and/or services

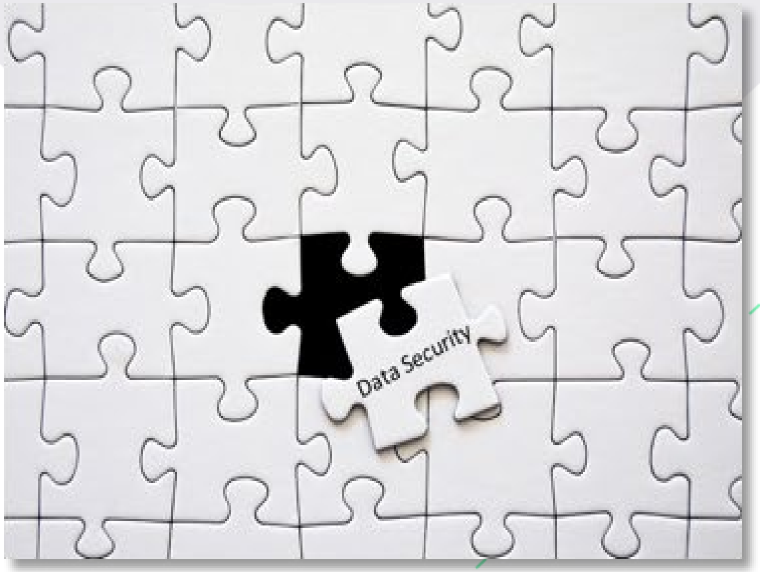
Plan, Design, Build, Deploy Models and Guidelines

Network, Computing Hardware, Operating Systems ,Storage, Security

With the *Zero Trust Network* paradigm, We Need a Zero Trust *Data Security Model to complete the picture*

Companies across nearly every industry are collecting and monetizing users' personal data. In return, they have to protect that data and make sure only authorized users can access it.

- data protects itself, everywhere and all the time
- data classification options to align with privacy and compliance
- robust policies to ensure governance compliance
- logging to support enterprise auditing and monitoring
- In-process inferencing to detect usage pattern anomalies



With the right data security model POSSESSION ≠ ACCESS!!

Fundamentals of Zero Trust Data Security

- Is the safety of your data dependent solely on the security of your network?
- If your infrastructure security is breached, would your data immediately be vulnerable to theft, manipulation, or destruction?
- Would a successful network break result in a successful ransomware attack?
- Would unauthorized possession of your data result in immediate access of that data?

Abstraction and Differentiation: Techniques for architecting Zero Trust Data Security.

When thinking about implementing a data centric approach consider two key requirements; Abstraction and differentiation.

- *Abstraction: Abstracting your data centric solution from infrastructure centric eliminates dependency and a potential for a cascade failure in the event of an infrastructure breach.*

- *Differentiation: Implementing a differentiated data centric solution from your infrastructure solution removes the adversary’s ability to use the same cyber tools, techniques, and procedures (TTP's) against your data centric protection.*

Abstraction and differentiation are two key cyber defense principles that can help you to create defensive layers that protect your data while operating in a high cyber threat environment.

About Trivalent:

Software Data Security company based in Annapolis, Md. *Focus Areas include Defense, Law Enforcement, Banking/Finance, Payment Processing and PAN data protection, Intellectual Property Protection, and Oil/Gas.*

- *Partnered with Keystone Security Group, SAS (Bogota/Manizales)*
- *Trivalent Contact:*
  - *Ricardo Bueno President/CEO*
  - *Email: rabueno@trivalent.us.com*
- Keystone Contact:
  - Juan Camilo Tresplalacios President/CEO
  - Emai: jctrespalacios@kestoneseg.com