



PKWARE[®]

**Mitigating the Risk
of Data Security Breaches**

**V. Miller Newton
CEO PKWARE**

Goals

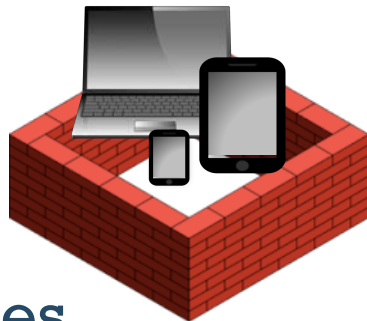
1. Define the enterprise information security challenge
1. Outline specific steps to address it
1. Q&A

2016 Breaches - Epidemic

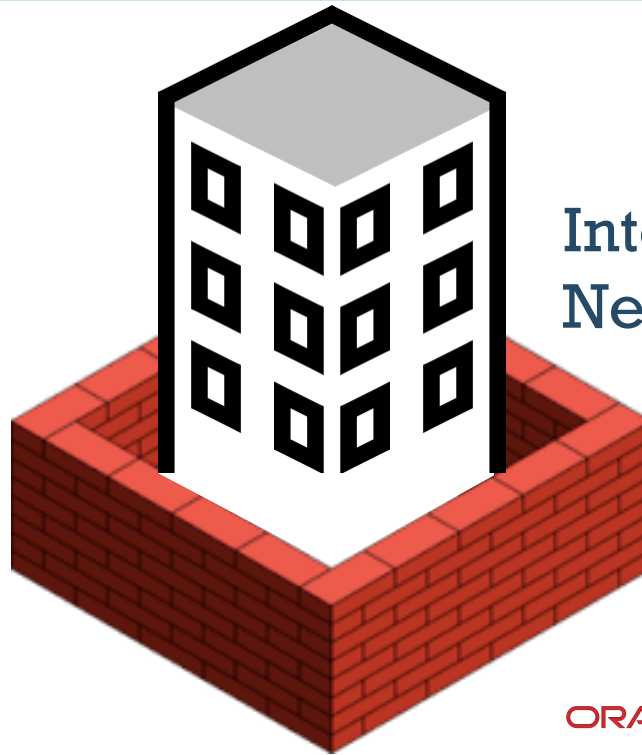


Enterprise Information Security

...Has Historically
Been About
Building Walls



Devices



Internal
Networks



Applications

But Data Can't Be Contained – It's Everywhere

SSN5867345596CCN2930440322934493DOB
05271972ID49504URGENT92304423ACCT98
43042IRS1040EZ1543003MLS5930445AUTH4
5909CONF9304540934AGENT903405ETA493
20435CODE234234345SSN5867345596CC29
30440322934493DOB05271972ID49URGENT
92304423ACCT9843042IRS1040E115430043
MLS5930445AUTH45909CONF93045409345
1AGENT903405ETA49320435CODE2342343
405_DATA_IS_EVERYWHERE_05271972ID4
9504URGENT92304423ACCT9843042I09IRS0

Data Itself Must Be Protected – With Encryption

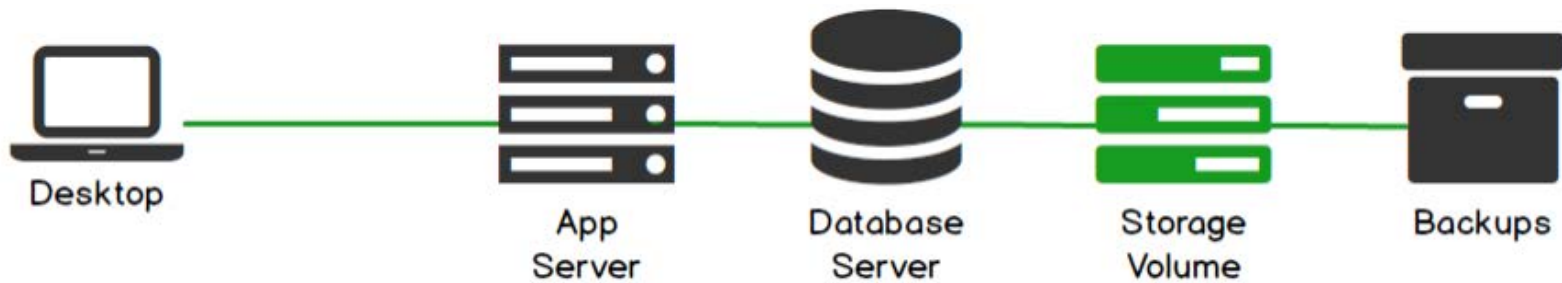
b0E/DO/0Lx/`g?MgzVI/!pfgx!/wg/?xg/`DO
/mfDVExgz!/`g/f?O/?/G0EI/0h/hVgOf/?zE/
G0zg/pf?p/DO/eV0xDhDgE/?zE/tgxhgmpg
E!/`g/V0MgO/LO!/`g/Wgg1O/WDpf/LO/Wf
gz/Wg/OLhhgx/?zE/xg:0DmgO/Wfgz/Wg/E
0/Wf?p/DO/xDefp!/`g/W?zpO/p0/m0ccLzD
m?pg/WDpf/LO</?zE/Wg/m?z/m0ccLzDm?
pg/WDpf/`Dc/pfx0Lef/ODzmgxg/tx?Igx!/`g/
f?Ogzmg/0z/pfg/g?xpf/O0/Wg/m?z/Vg?xz/
?z **ENCRYPTION PROTECTS** E/ex0W!/0/
eDMgz/LO/pfDO/>gz!/`g/f?O/?/G0EIgz!/`gs

Encrypted?: What Google Says...

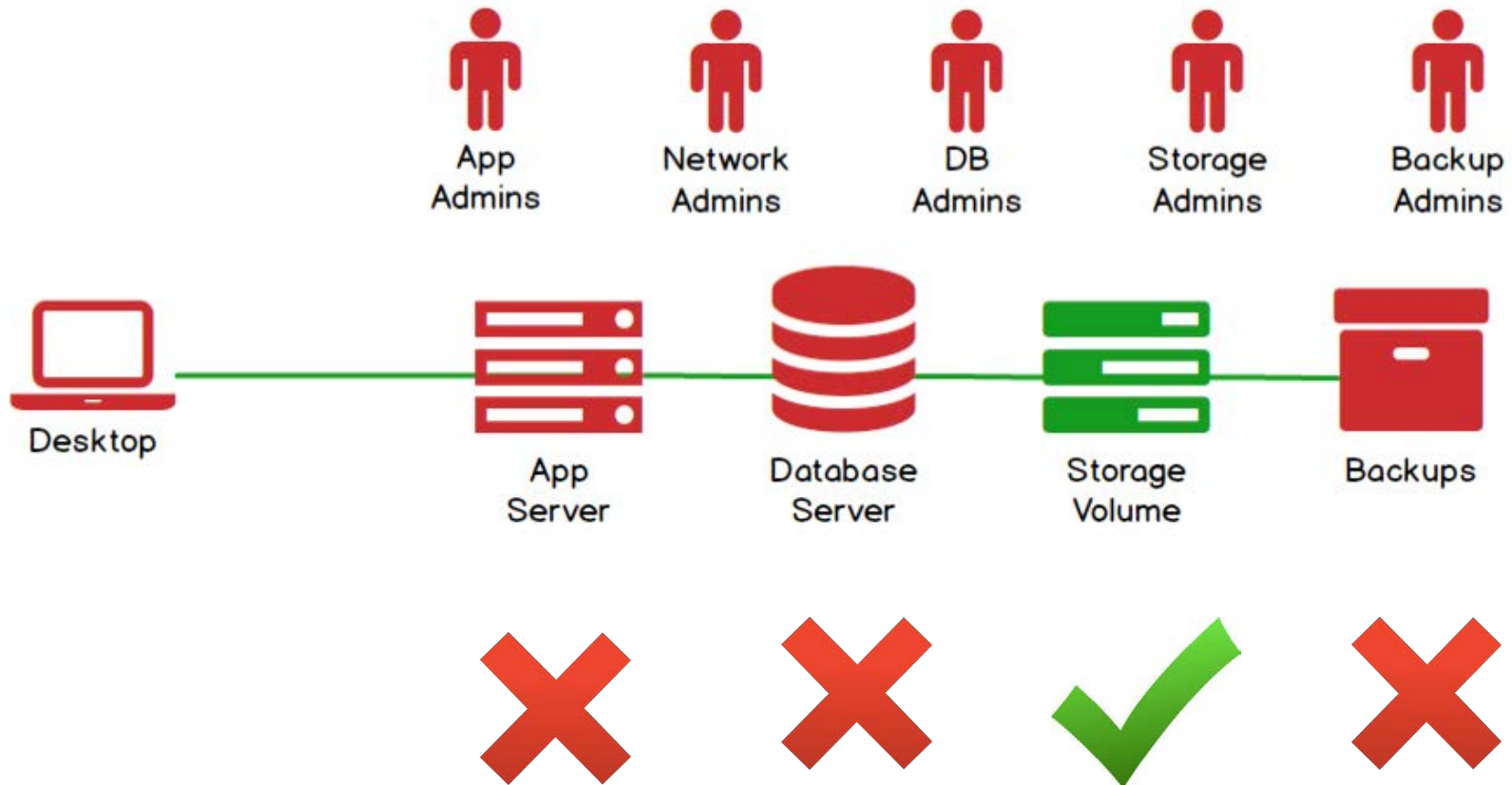
Does Google encrypt my data?

Yes. Data is encrypted at several levels. Google forces HTTPS (Hypertext Transfer Protocol Secure) for all transmissions between users and G Suite services and uses Perfect Forward Secrecy (PFS) for all its services. Google also encrypts message transmissions with other mail servers using 256-bit Transport Layer Security (TLS) and utilizes 2048 RSA encryption keys for the validation and key exchange phases. This protects message communications when client users send and receive emails with external parties also using TLS.

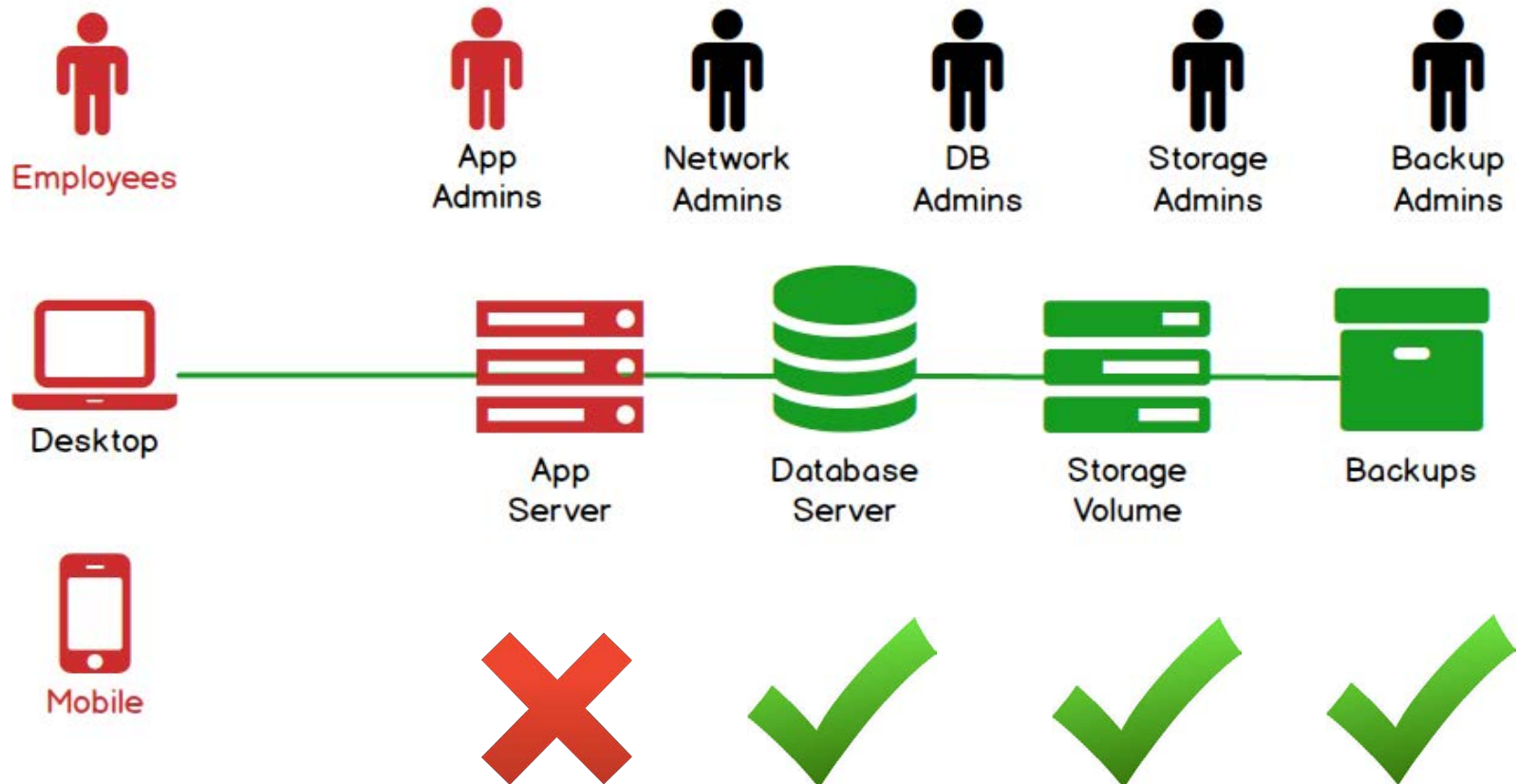
Encrypted?: What Google Means



Encrypted?: What Google Means



Encrypted?: Top 5 US Bank Better, But...



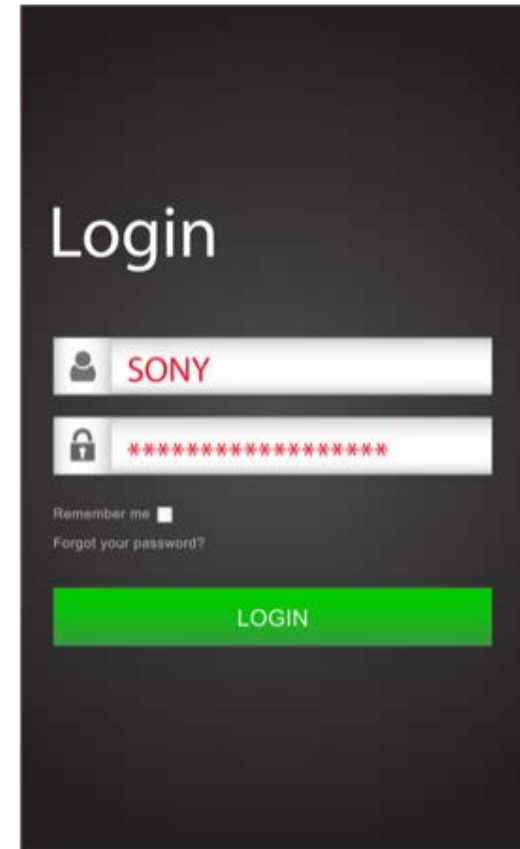
Who Do We Actually Need to Protect Against?



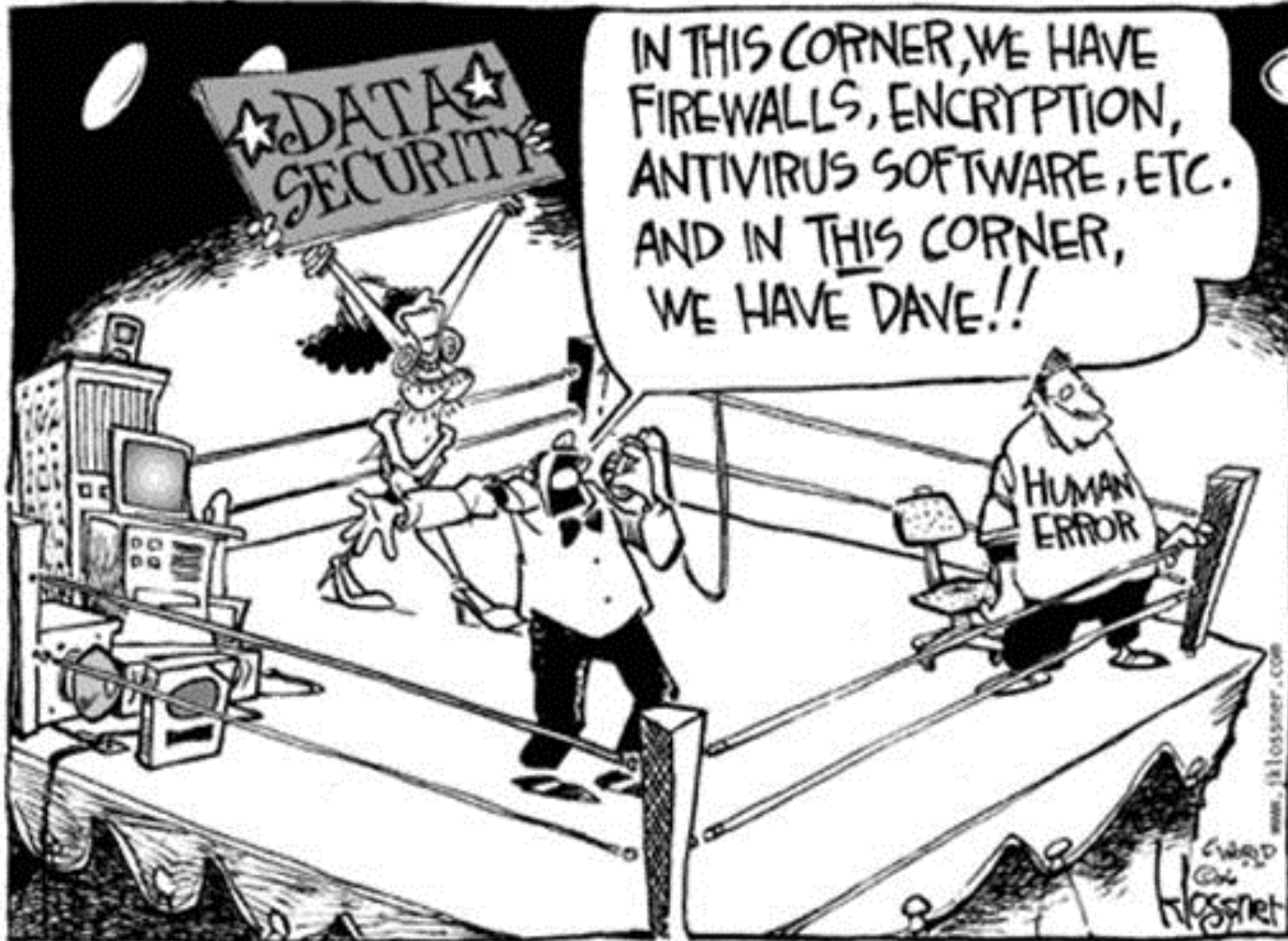
Thieves – Nefarious Outsiders



Snoops – Legitimate Access Goes Rogue

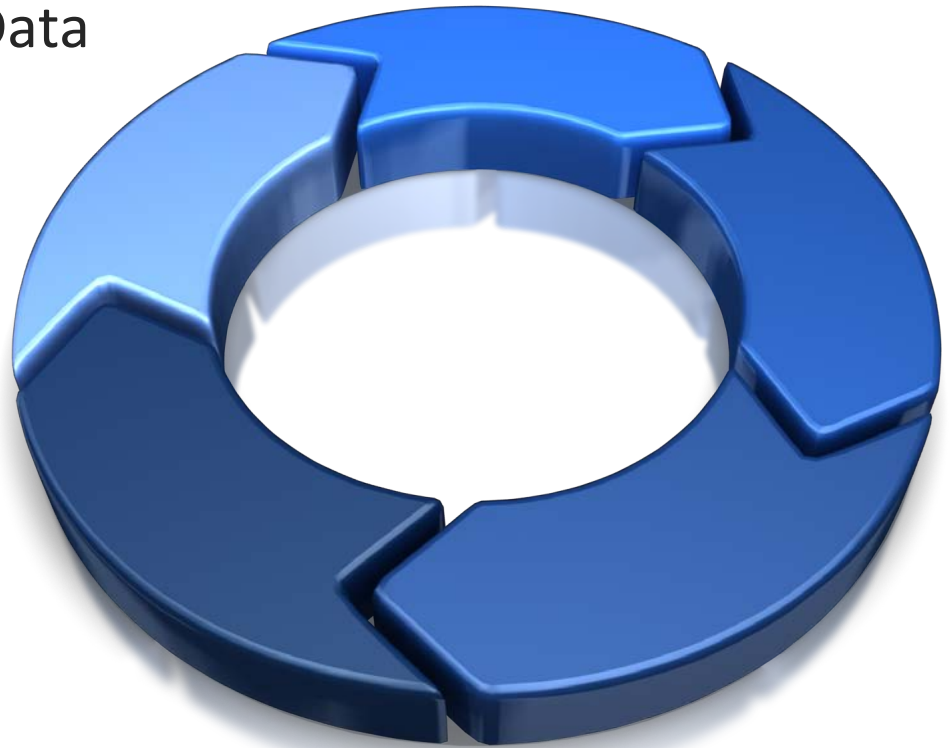


Idiots – Helpless, Hapless Insiders



5 Steps To Protect Your Enterprise

1. Designate a Data Protection 'Officer'
2. Discover Your Sensitive Data
3. Determine Your Gaps
4. Define Your Policies
5. Deploy Protection



1. Designate a Data Protection 'Officer'

- Who is the one individual responsible for data security in your company?
- Is it a business person or a technology person?



2. Discover Sensitive Data

- What types of sensitive information does your organization handle?
- Where does it reside?



3. Determine Data Security Gaps

- Who has access to your sensitive information?
- What controls are already in place?
- How much visibility do you have?



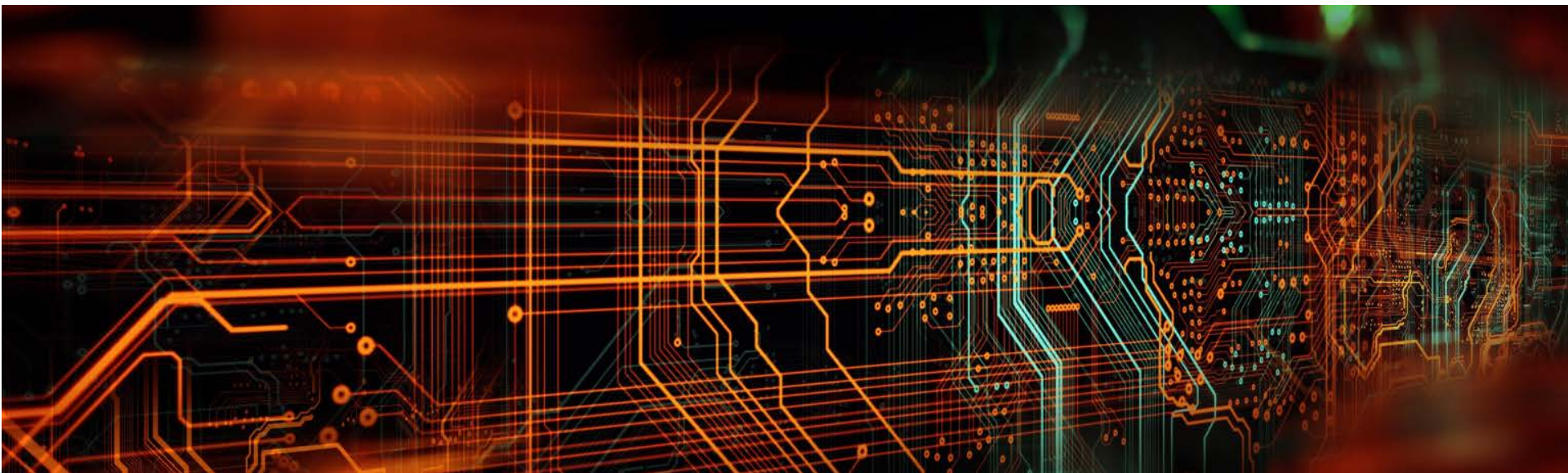
4. Define Data Security Policies

- Who should have access?
- Who should control and audit access?
- How should duties be separated?
- What are your stakeholder requirements?



5. Deploy Persistent Protection

- How will data be protected...
 - At rest?
 - In motion?
 - In use?
- How will data security be reported, audited & verified?



Conclusion

- ❑ Enterprise data itself must be protected, not just networks, systems and devices
- ❑ Encryption needs to be persistent – following data everywhere it is used, shared or stored
- ❑ Enterprises need to maintain exclusive control of their encryption keys
- ❑ Data protection needs to focus equally on people, process, and technology in order to adequately protect against thieves, snoops & idiots



PKWARE[®]

**Mitigating the Risk
of Data Security Breaches**

**V. Miller Newton
CEO PKWARE**