



plante moran | Audit. Tax. Consulting.
Wealth Management.

Building a strong platform strategy: IT and cybersecurity implications

November 15, 2018



Today's Presenters



Craig Zampa

Principal, technology consulting

craig.zampa@plantemoran.com

248-223-3703

[Learn more about Craig](#)



Mike Lipinski

Principal, cybersecurity consulting

mike.lipinski@plantemoran.com

248-223-3259

[Learn more about Mike](#)



About Plante Moran

Plante Moran is one the nation's largest certified public accounting and business advisory firms providing tax, audit, transaction advisory, technology, operations, and strategy services.

1924

year founded

3,100+

professionals

26

offices

20,000+

clients

1,500+

private equity and
portfolio company
clients

10

affiliates including
investment bank,
PMCF



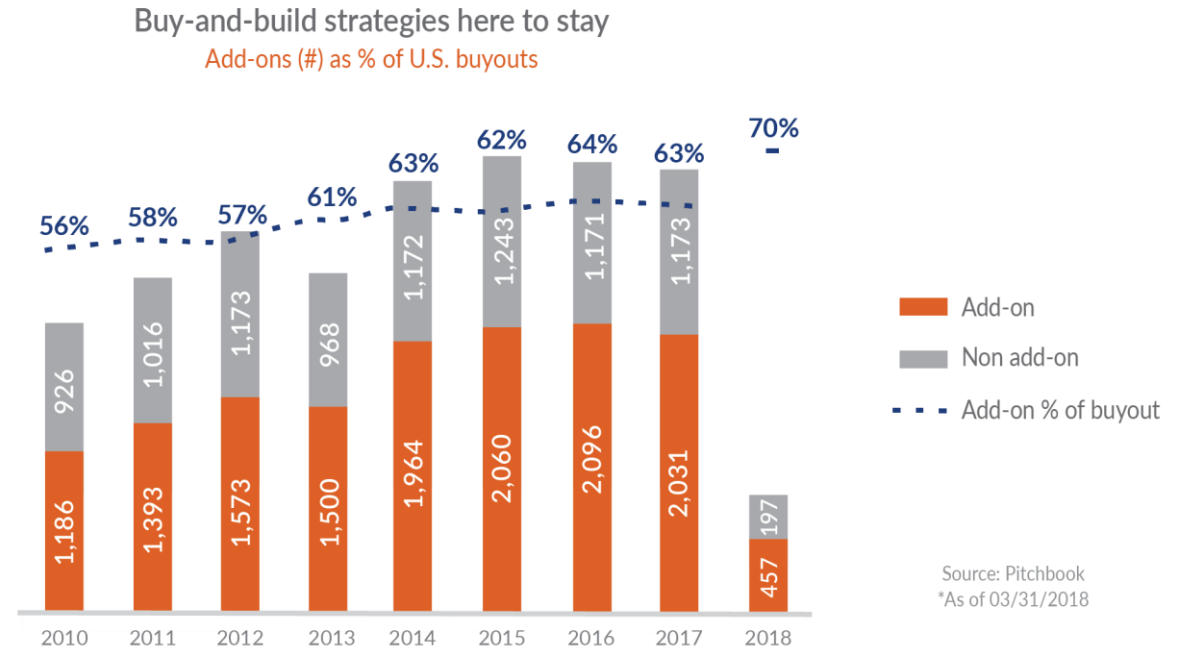
Key objectives

- Identify key considerations when building an effective platform
- Understand the critical IT and cybersecurity elements related to platform investing
- Implement an IT and cybersecurity risk mitigation strategy.



Portfolio to platform

- Add-on volume increase
- Common to see add-ons prior to platform strategy
- Develop and communicate investment thesis early





Polling question

How many platform investments/add-on acquisitions have you executed over the past three years?

- 0
- 1-5
- 6-10
- 11+



Start with strategy



Set the platform growth strategy



- Where and how?
- Product and service expansion?
- Centralize operational teams?
- What will be the management or resource gaps?



Set the IT/cybersecurity strategy

- Structure IT/cybersecurity leadership and PMO
- Governance
- Plan IT support and service providers
- Rationalize and centralize business applications



Set the IT/cybersecurity strategy

- Perform infrastructure and cybersecurity gap analysis
- Develop key IT/cyber policies, procedures, and standards (i.e. support, on-/off-boarding, hardware)
- Develop detailed improvement and future assimilation plan



Considerations & gaps



IT considerations



- Current tools and resources adequate?
- Employ people and tools for “future state”
- Does cloud technology fit into the strategy?
 - Elastic IT to support growth
 - Time zone impact
 - Reduced disruption impact
 - Cloud platform considerations



Cybersecurity considerations

- Will add-on strategy introduce new regulatory compliance issues?
- Mobility considerations for decentralized/deployed users
- Cloud security strategy
- Privacy regulations
- Fraud/Insider threat
- Cybersecurity resilience
- Devaluation for a cyber event



Identify critical gaps

Strategic



- Risk assessment
- Regulatory/compliance
- Policy/procedures
- Budget & planning
- Staffing
- Training
- Vendor management program
- Incident response capabilities

Operational



- Technology capabilities/limitations
- Service level agreement (SLA) best practice
- Key performance indicator (KPI) best practice
- Business continuity planning verification & testing

Tactical



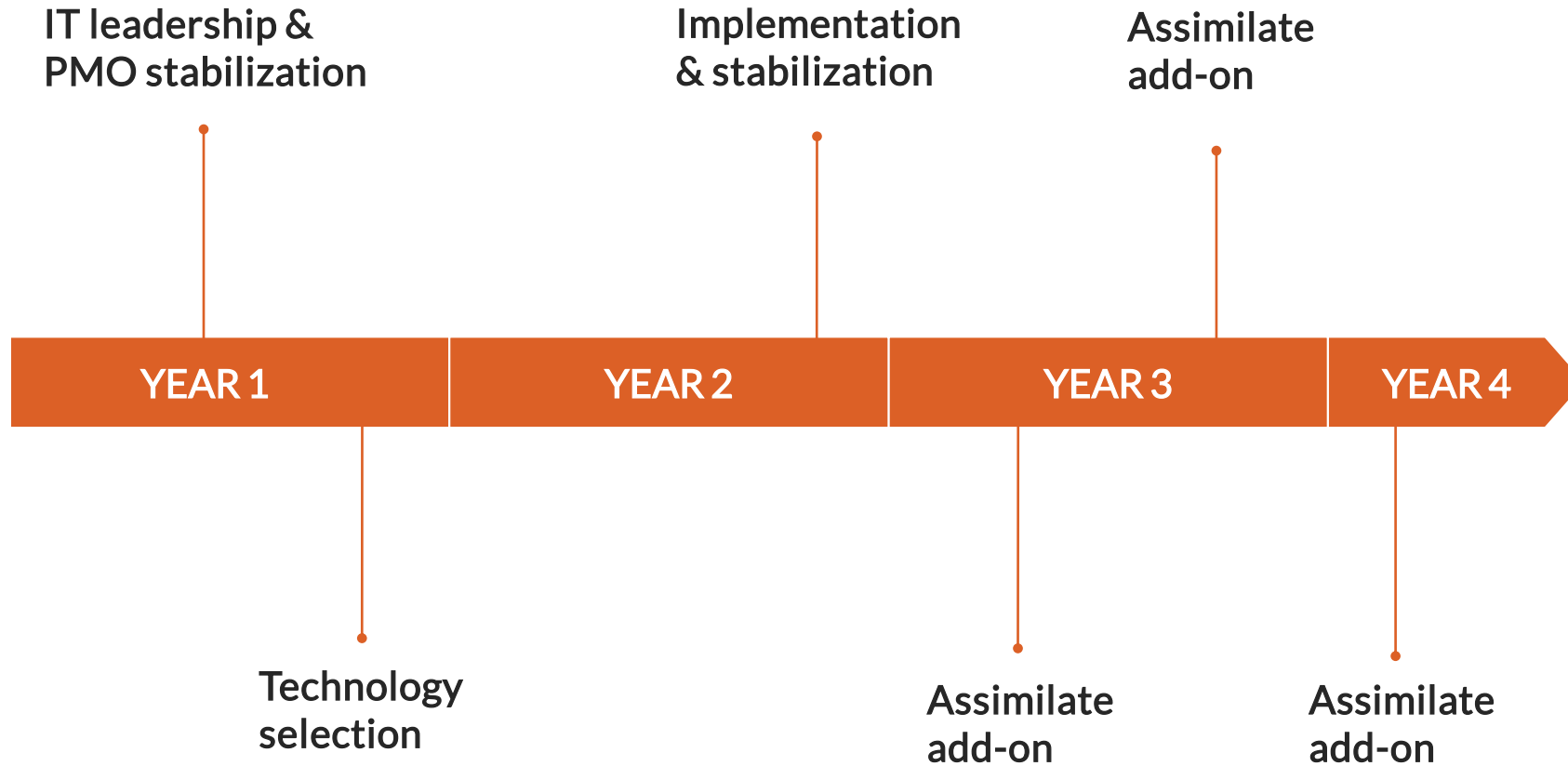
- Scalable/effective
- IT & cybersecurity testing
- Vulnerability issues
- Logging & monitoring



Importance of the right timing



Know the timing





Manage for risk

- External firms can help but dedicate internal assimilation team
 - Build roles within an assimilation charter
 - Backfill resources as needed for appropriate commitment
 - Add-ons cannot assimilate themselves, provide leadership and presence from central business
- Every platform is unique, avoid cookie-cutter approach
- Invest upfront to avoid reduced value at exit



Questions

Craig Zampa

Principal, technology consulting

craig.zampa@plantemoran.com

248-223-3703

Mike Lipinski

Principal, cybersecurity consulting

mike.lipinski@plantemoran.com

248-223-3259