



EARNING CUSTOMER TRUST

PRESENTED BY BRYAN CULP
NOVEMBER 8TH, 2024
ISC² EAST BAY CHAPTER, CYBER
IN GRC CONFERENCE

Current Responsibilities... aka *Point of View*



Customer Trust – provide customers with assurance info + documentation... “customer assessments”



Third Party Risk – review vendor assurance info + documentation... “vendor assessments”



Policy Program – establish and work with business owners to update and get approval for policies + SOPs



Management Review – cross-functional leadership forum to review business metrics + address issues

When you have a policy,
but no actual controls





**TRYING TO ENSURE
YOUR COMPANY MEETS
SOC 2, ISO 27001,
HIPAA, HITRUST,
PCI-DSS, FEDRAMP, CMMC
AND PRIVACY REQUIREMENTS**

THE GRC TEAM

Customer Trust is growing because of customer demand



Customer Trust responsibilities – an example



Customer Questionnaires

Traditionally security questions – now broader and often via a third-party portal

- Complete customer questionnaires
- Manage customer Salesforce request queue
- Respond to one-off slack channel requests
- Maintain industry standard templates (SIG, CAIQ, HECVAT, etc.) to share in place of customized questionnaires



Customer Audits + Meetings

Relatively rare – virtual audits based on contractual audit rights and live 'assurance' meetings

- Security policy audits
- Evidence audits
- General 'assurance' meetings for select large customers
- Follow-up conversations regarding customer findings/recommendations from security questionnaires and audits



Content Distribution + Creation

Going beyond the distribution of controlled docs to curating content – especially with the advent of AI

- Trust Center on public website
- Controlled document distribution (SOC 2, Penetration Tests, etc.)
- Knowledge Papers
- Data repository Q&A pairs
- Internal Resources

Current reality of Customer Trust

Customer Trust

- Provide templates when can
- Use 'trust package' for lower TAV
- 3rd party platforms 50%+ of asks and come in *many* varieties
- High TAV contractual audit rights
- Bottom line: Ongoing burden shift to Customer Trust side
- AI holds the promise of being an automated 'universal translator'



Third Party Risk

OneTrust

servicenow

ProcessUnity

whistic

AUDITBOARD

- Significant pressure to ask more questions + get more info
- No CSP onsite audits or info on / access to 'fourth parties'
- Perception that VC investment going to third-party risk side of the trust equation, *not* Trust
- Proliferation of start-ups offering bespoke customization and comparative analytics

The Future of Customer Trust



Customer Trust is becoming a **recognized function** – regardless of name or org design



Automated scaling of vetted, secured info between Customer Trust (vendor) and Third-Party Risk (customer)... *is coming*

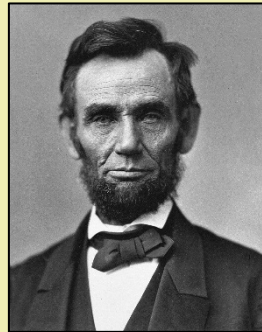


Continuous Monitoring is *still* the future –select sharing of secure, real-time info and metrics *will* happen

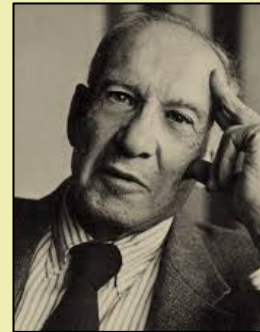


Wolf of Wall Street

“The best way to predict
the future is to create it.”



Abraham Lincoln
1809-1865



Paul Drucker
1909-2005