Outside the ivory tower

How security teams can support radical change & digital transformation

STEVE DAVIES

About Me

Steve Davies

linkedin.com/in/sldavies

twitter.com/northvein

Senior Manger, Cyber Security at DLA Piper (International)

- Enterprise Security Architecture & Engagement
- Security Operations & Engineering

Enterprise Security Architect at Sky Betting and Gaming

Security Architect at William Hill

Introduction

Context

- Organisations were in a fight for survival before the pandemic, now they’re rushing to modernise and innovate faster than ever before
- Many are now in a period of *radical change* which will see them try to adopt digital technologies to:
    - improve business processes
    - improve their products for their customers
    - modernise the workplace in a late-stage/post-pandemic world
- With every significant technical changes comes an associated cultural and organisational cost contributing further to disruption

Introduction

Context

- Organisations already have enough to work through, how to be secure is one less thing they should need to worry about
- Security is no longer a new problem - most organisations have had a security team for a decade or longer
- Security teams can and should be doing more
- Security teams should be pitching in and no longer coaching from the sidelines
- Security teams should have skin in the game when it comes radical change and digital transformation

We can help

Here’s why

- We have a broad and deep understanding of the business, how it works and its requirements
- We’re well schooled in thinking in business terms to ask, ‘why are we doing this?’/ ‘what are we trying to achieve for the business?’
- We’ve been developing our stake holding and communications skills for a decade+
- We’re used to constantly explaining, educating, debating and selling ideas, as well as influencing people
- We’ve got the strength of character to stand up to those who lack understanding or an appreciation for the bigger picture

We can help

Here’s how

- We need to get out of the ivory tower

ivory tower

noun

a state of privileged seclusion or *separation from the facts and practicalities of the real word*

Security Teams

In the real world

- Security teams can have a reputation of being difficult to work with, even aloof
- Security teams can sometimes be removed from whatever it is the business does
- There are reasons for this historically, and they should retain some independence, but….

- Our customer is the organization
- Our customer could be the customer too,
    - the services they’re now transforming are underpinned by the services we helped them to secure
    - re-use a lot of the security we’ve worked to build into the organisations own people, processes and technologies

- After a decade+ of infosec, there is a broad consensus that security works better the further left it shifts
- Security works better when its people, processes and technologies are aligned with what the organisation is doing for the customer

How do we

Do More?

- How do we get out of the ivory tower?
- It’s going to be different for every organisation but at a high level, all security teams will need to;

ivory tower

noun

a state of privileged seclusion or *separation from the facts and practicalities of the real word*

HOW SECURITY TEAMS CAN SUPPORT

RADICAL CHANGE & DIGITAL TRANSFORMATION

CULTURE

Revisit where security lives in the organization & reinforce partnerships across the business

CATALYST

Challenge long established beliefs around risk to provide aircover for innovation

COLLABORATION

Reshape the security team to better support rapid and radical change

COMMITMENT

Switch from a ‘No’ to a ‘Yes, here’s how’ culture

COMPLIANCE

Modernise assurance & compliance for internal and external stakeholders

CULTURE

Revisit where security lives in the organization & reinforce partnerships across the business

- Security is still often perceived as an expensive IT problem
- Whilst making progress we still have to elbow our way into many conversations
- Risk, Compliance and Procurement often lack visibility and struggle with engagement

- Radical change and digital transformation have technology at their core
- Security has spent a decade+ working closely with IT and technologists
- The security team is likely to already have relationships with technology teams which Risk, Compliance and Procurement do not

- We need to shift left, closer to our customers and do more for them than we ever have before
- We need to reinvest in our partnerships to ensure nobody is left behind

CULTURE

Revisit where security lives in the organization & reinforce partnerships across the business

Provide psychological safety

- Security teams need to make sure everyone knows that no matter what happens, the security team will have their back
- In return for stake holding and engagement, this provides the safety needed for transformation and innovation to happen

Aggressively challenge and eliminate conflict with existing partners

- The relationship with other teams may have become toxic over time, even tribal
- Security teams need to reboot their thinking, not treat business partners as adversaries and trust that everyone is trying to do the right thing
- Security teams should democratise responsibility and invest in verifying outcomes rather than controlling people and processes.

CULTURE

Revisit where security lives in the organization & reinforce partnerships across the business

Build the support network

- Security teams need to leverage their relationships with other support functions and provide them with a means of surfacing and satisfying their requirements
- In representing Risk, Compliance, Procurement etc. the security team can reduce the need for multiple conversations in parallel, typically with teams that lack technical SMEs
- By acting as an interpreter of sorts, technologists can focus on developing and delivering in confidence that these requirements will surface in a familiar format
- As and when risks & issues come to light, the whole group knows that they can work to the assumption that the security team will report and track these issues (so they don’t have to)

CATALYST

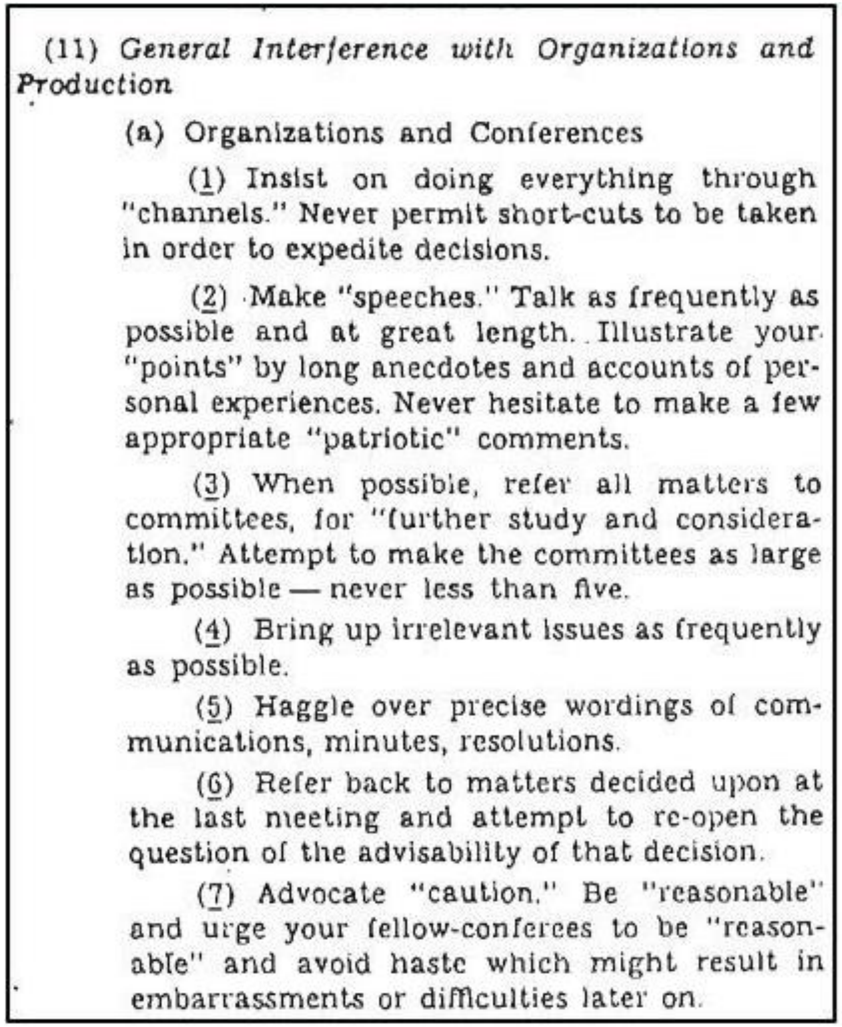
Challenge long established beliefs around risk to provide aircover for innovation

- Risk management is often misunderstood or even mysterious
- Any change which fundamentally disrupts how the organisation works is going to result in nervousness
- Any change involving new technology or changes to where data resides will result in calls for prudence, caution and some sort of risk decision
- It’s not uncommon to see service owning teams delay or throw out changes because “security won’t allow this”

- We need to exercise our own authority to approve what we can
- We need to remove all ambiguity around how we are going to handle risks and source those approvals for making radical changes and transforming services

CATALYST

Challenge long established beliefs around risk to provide aircover for innovation



(11) *General Interference with Organizations and Production*

(a) Organizations and Conferences

(1) Insist on doing everything through "channels." Never permit short-cuts to be taken in order to expedite decisions.

(2) Make "speeches." Talk as frequently as possible and at great length. Illustrate your "points" by long anecdotes and accounts of personal experiences. Never hesitate to make a few appropriate "patriotic" comments.

(3) When possible, refer all matters to committees, for "further study and consideration." Attempt to make the committees as large as possible — never less than five.

(4) Bring up irrelevant issues as frequently as possible.

(5) Haggle over precise wordings of communications, minutes, resolutions.

(6) Refer back to matters decided upon at the last meeting and attempt to re-open the question of the advisability of that decision.

(7) Advocate "caution." Be "reasonable" and urge your fellow-conferees to be "reasonable" and avoid haste which might result in embarrassments or difficulties later on.

CATALYST

Challenge long established beliefs around risk to provide aircover for innovation

Ownership

- Security teams need to own risk management to support radical change and digital transformation
- Security teams need to be the risk person in the room to ensure tight feedback loops and quick decisions on issues
- The Security team can usually ‘sign-off’ on so much - and they should
- The Security team should work with the wider risk management function (if it exists), removing the need for their day-to-day
- The Security team should be responsible for planning and producing evidence around how risks were identified and managed before, during and after any transformation / migration

CATALYST

Challenge long established beliefs around risk to provide aircover for innovation

Vendor Risk Management

- The importance of Supplier Risk management and its maturity cannot be understated
- The Security team need to ensure Supplier Risk Management is considered and that their approach makes sense in a world where 3rd/4th parties have increasing reach and responsibilities

Groundwork

- Security teams need to be able answer difficult questions with details and requirements
- Security teams need to engage with Privacy, Compliance and legal teams in advance
- Security teams need to establish the guardrails for transformation and demonstrate how these adequately address concerns in advance

COLLABORATION

Reshape the security team to better support rapid and radical change

- Security teams often have little operational responsibility within the organisation
- Security teams are often engaged in a project support capacity (security architecture) and then in a limited on-going capacity (security operations, compliance etc.)

- Engaging security teams can often feel like working with an external party
- Getting the security team to take on more responsibility can often be a difficult conversation

- Security teams are often unprepared to extend their remit to an organisations customers in receipt of new products and services built on a technology stack that once served only the organisation
- Security teams can get ‘wrapped around the axle’, focusing too much on the risks around moving to cloud or transforming services whilst ignoring the immediate

COLLABORATION

Reshape the security team to better support rapid and radical change

Cloud Centre of Excellence / Transformation Steering Groups

- Security teams should be instrumental in the formation of CCoEs or Steering groups that form to serve the organisation. Supporting these through adequate representation and resource better serves all customers whilst dissolving historical boundaries
- Security teams should be instrumental in the supporting business case and thinking around transformation and modernisation. Providing clarity around the benefits, from a risk and security perspective, will add weight to the collective vision and ensure the security team is re-framed as an enabler

COLLABORATION

Reshape the security team to better support rapid and radical change

Security Services

- Security teams need to go beyond project engagement to support radical change
- In addition to Security Monitoring (SecOps, SOC), we need to make Security Engineering a consumable service
- In addition to traditional services like vulnerability management, Security teams should look to take on more of the burden by managing day-to-day concerns like Identity and Access management
- Security teams should re-engineer existing and design new services with modern provisioning and consumption methods in mind, removing the need for manual processes wherever possible
- Security teams should describe a roadmap for providing these services, along with timescales. The CCoE should be able to rely on these dependencies
- Security teams should be a part of the shared responsibility discussion and should

COMMITMENT

Switch from a ‘No’ to a
‘Yes, here’s how’ culture

- Security teams often have a reputation for saying no
- Processes for managing change can sometimes reduce security input to an approval

- Security teams often obstruct change without providing guidance or alternatives
- Security teams can sometimes focus on risk elimination rather than risk management

- Security teams can often be insular, or in extreme circumstances, tribal
- Security teams don’t often contribute to solutions outside their wheelhouse

COMMITMENT

Switch from a ‘No’ to a
‘Yes, here’s how’ culture

Make time

- Security teams need to commit time, people and resources to supporting radical change
- Security teams need to plan and promote L&D to ensure they don’t lose SME status

Lead by example

- Security teams have (probably) already migrated and transformed services of their own
- Security teams can share/demonstrate their approach and help set the tone around risk appetite

Be Supportive

- Security teams are in a prime position to serve as digital tour guides, and help

COMMITMENT

Switch from a ‘No’ to a
‘Yes, here’s how’ culture

Share

- Security teams should share their success stories and their failures, internally and externally
- In addition to evangelising the new ways of working, visibility will help attract and retain talent

Do some of the heavy lifting

- Security teams should take on some of the big challenges themselves and help build the future operating model
- Security teams can always start something and hand it over to IT/Service teams later for operation

Promote the engineering mindset

- Focus on real problems and engineering solutions to these first rather than drawing together a long list requirements

COMPLIANCE

Modernise assurance & compliance for internal and external stakeholders

- Compliance can be confusing and even controversial
- A lot can be said about the differences between security and compliance
- In practice we have to demonstrate compliance and many organisations are likely to have a framework for managing this with existing processes and reporting
- These efforts are often manual and resource intensive
- One of the biggest benefits of digital transformation is the chance to modernise compliance and assurance activities
- Radical change may be the first, last and only chance we ever get to redesign and simplify these processes
- Radical change provides us with the opportunity to do away with mandrolic assurance and reporting activities

COMPLIANCE

Modernise assurance & compliance for internal and external stakeholders

Capitalise on the Opportunity

- Security teams need to sell and own the delivery of enhancements around assurance and demonstrable compliance for internal and external stakeholders
- Security teams should engage with customer/client engagement teams to ensure they too can benefit from these in support of pitches and sales
- Security teams need to extract the same level of detail and demonstrate the same level of care for SaaS services where such details can be obscured. This might be as simple as recycling their own supplier risk assessments
- Security teams need to consider and reposition compliance as an outcome

Thanks

GET IN TOUCH

linkedin.com/in/sldavies

twitter.com/northvein

SEPTEMBER 16 VIRTUAL EVENT

15TH SECURING THE LAW FIRM

SECURING THE LAW FIRM VR

LESSONS IN LEGAL CLOUD MIGRATION PANEL DISCUSSION

Sue Diver
Head of Information Governance,
Simmons & Simmons

Steve Davies
Senior Manager - Cyber Security,
DLA Piper

Rhiannon Jones
Director, Cyber practice, & UK Data Protection & Privacy lead
EY

Jonathan Freedman
Head of Technology & Security,
Howard Kennedy

Register as a guest @ https://akjassociates.com/event/stlf