SAP Enabling Trust & Embedding Security

Paul Greif,
Director,
Customer Information Security Advisor, Chief Trust Office, SAP Global Security Group,

Sandip Dholakia, *Member Infragard*
CISSP, CCSP, CCSK, GWAPT, AWS Security Specialty
Principal Security Architect, Chief Trust Office
SAP Global Security Group,

Agenda

- About SAP Chief Trust Office

- Threat & Threat Landscape

- Challenges with Trust

- SAP Chief Trust Office Solutions to Challenges

- Q & A

If the lifeblood of the digital economy is
Data,
then the HEART of the digital economy is
Trust!!

-*PWC Digital Trust Insight*

Chief Trust Office Mission

- Purpose: To preserve the trust of our global customers and partners by developing an internal governance framework focused on security, transparency and privacy.

- In our organization, we challenge ourselves to deliver on our core focus of **defending our organization and our customers,** against cyber threats on a daily basis. The **SGS Chief Trust Office** is providing our global customers and partners with the resources they need, so they can easily know how their workflows and data are protected and reach out to us

- As technology markets continue to evolve globally, we seek to differentiate on **trust and transparency** in addition to quality of products and services, agility and engagement with our stakeholders. We are now increasing our scope and strategic responsibilities as an **organizational catalyst** in this important differentiation and development.
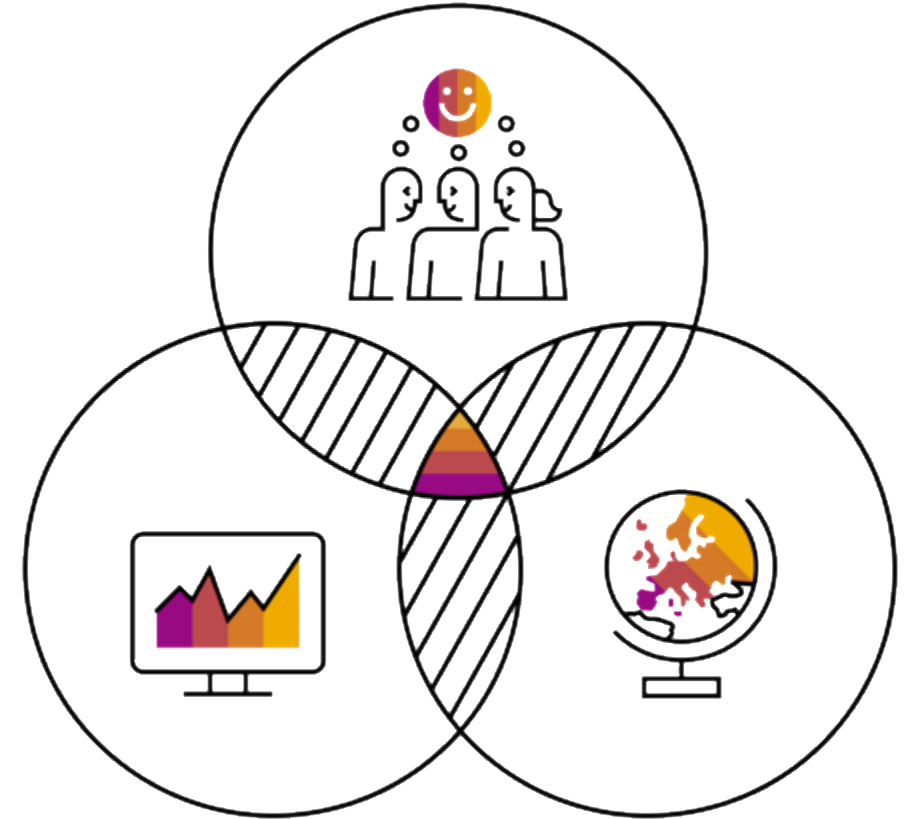
Chief Trust Office Vision and Commitment

Demand for issues around trust continues to grow in the marketplace, particularly around cloud security, we strive for market excellence by:

- Strengthening trust with our customers and cloud technologies by building **a strong security foundation**

- Provide **seamless communications** between our business units

- Greater transparency to our customers to foster **trust and long-term relationships**

- Shaping the global security narrative by **pushing the limits on setting industry standards**

OUR COMMITMENT

SGS Chief Trust Office has been established **to set the global security and privacy narrative**. We aim to drive core leadership in setting responsible policies, frameworks and policies to serve our **200 million SAP users worldwide**

Chief Trust Office **Functional Areas**

Secure Development Operations:

Drive security learning curriculum across employees and contractors and focus on developer security mindset and culture

Improve the delivery, efficiency, and retention of security knowledge

Customer Information Security Advisory:

Enable SAP customer facing roles to "sell" the Security and Data Protection of the SAP Cloud solutions as an additional asset

Enables SAP Field organization with readily available customer facing Cloud Security and Data Protection documentation

Process Automation & Enablement, Regulatory Compliance & Governance:

Improve processes and operations across CTrO by streamlining manual procedures

Improve security architecture, develop content workflow, gap analysis, and user testing

Research on frameworks, standards, certifications, policies

Chief Trust Office **Functional Areas**

Global Customer Engagement:

Events, customer-facing, internal knowledge enabling

Promote SAP's security message through events and educate employees about SAP's security strategy internally

Connect likeminded individuals within the security organization and promote personal develop and learning

Content Development:

Create resources for customers, internal stakeholders, and the public to learn more about SAP's security practices, policies, and processes;

Includes blogs, white papers, newsletter articles, videos, and other messaging about security topics that relate to our customers and partners

Security Architecture:

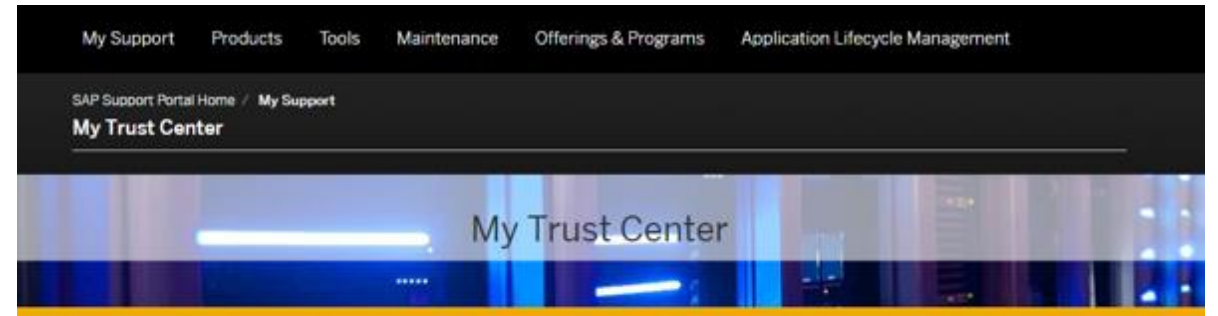Provide guidance on security features and cloud environments in line with SGS requirements

Operations:

Support day-to-day operations of the teams in the Chief Trust office

Deliver projects and content and ensure leadership has the support they need to push team strategy forward

Content Development What is SAP My Trust Center?

- Provides classified, detailed information and resources about SAP's **Security, Data Privacy, Compliance and Agreements**

- Hosted in **SAP Support Portal**

- Includes **subscription functionality** that notifies subscribers about content updates

- Only accessible to **customers and partners with valid S-User ID**

My Trust Center Components

Policies, Frameworks, and TOMs

- Technical and Organizational Measures

- SAP's Security Controls and Measures

- Global Security Policy (multiple languages)

Sub-processors

- LoB-focused lists of sub-processors

- Description of provided services and location

- Subscription available

Compliance Documents

- Evidence documents from SAP partners providing services t SAP

- Data Center facility service, Infrastructure as a Service, Cloud Solution Extension services

Tools and Documentation

- Reference guides, white papers, service and support documents

- Global Security, Cloud Services and Customer Information

Threats & Threat Landscape

- Threats – *just to name a few*

Data Breaches & Data Loss	**Compromised Credentials**
Application Vulnerabilities	**Hacked Interfaces and Insecure APIs**
Denial of Service Attacks	**Malware**

Motivations are unlimited – money, espionage, competitor info…

Software and applications are becoming extremely complex

Every device & every app is increasing the threat surface!!

Attack surface of your organization is much larger than you have ever imagined

Today's Threat Landscape

36B Records exposed by data breaches

58% Of breaches involved personal data

40% Growth of ransomware attacks during the pandemic

6.95M New phishing and scam pages created

68% Of business leaders feel their cybersecurity risks are increasing

$3.86M Average cost of a data breach

28% Of organizations reported having ransomware during lockdown

55% Of data breaches are deployed by organized criminal groups

Impact of Cybercrime

Economic Impact

- Theft of corporate information, intellectual property and customer data
- Interruption of commercial activities
- Repair costs of damaged systems

Reputational Impact

- Massive loss of trust
- Customers moving to the competition
- Negative media coverage

Regulatory Impact

- Regulatory fines and sanctions due to GDPR and data breach laws

The damage related to
Cybercrime
is projected to hit
$6 trillion USD
by 2022

People are the
weakest link

More than 90%
of attacks are result of
Compromised Credentials!!

Best Practices

✓ Shift Left – Embed security at the design phase

✓ Hardening – Update/patch OS and Software

✓ Access Control – Review and manage access

✓ Data protection – Encrypt or Mask data

✓ Monitor – Collect and analyze data

Trends in Cybersecurity

❑ Implementing Zero Trust Architecture (ZTA)
- o Multifactor authentication
- o Micro-segmentation
- o Granular access

❑ Combat Ransomware –
- o Perform regular and multilocation backups

❑ Use of AI/ML to parse & hide the sensitive data

❑ Enhanced logging & monitoring capabilities

State of Trust
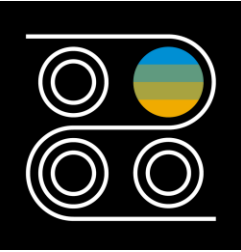
Concern about future of work due to automation
83% of respondents

Governments can't regulate fast enough
61% of respondents

Technology makes it difficult to identify "fake news"
75% of respondents

70%
Of consumers feel that **businesses haven't done enough** to safeguard their personal information

59%
Of buyers are likely to **avoid companies** that suffered from a cyber attack in the past year

25%
buyers tend to **abandon products and services** in favor of a competitor after a single ransomware-related service incident

Challenges of Trust Office

1 Transparency
-- Customers need information / updates

2 Access
-- Customers want easy access to info

3 Mistakes
-- Customers expect honest explanation

4 Goal
-- Customers' goal is to keep data secure

5 Right
-- Right to choose what to share

We at SAP are
very
Serious About Security!

- Dedicated **Trust Office** – part of SAP Global Security Group. Led by **Chief Trust Officer Elena Kvochko**

- SAP Cyber Defense Center – innovation hub for new cyber defense capabilities

- SAP Chief Security Officer – reporting directly to our CEO Christian Klein

Challenges of Trust Office

1 Transparency
-- Customers need information / updates

2 Access
-- Customers want easy access to info

3 Mistakes
-- Customers expect honest explanation

4 Goal
-- Customers' goal is to keep data secure

5 Right
-- Right to choose what to share

SAP Solutions to Challenges

1 Websites, Whitepapers, Blogs and more

2 SAP Trust Center, Patch Tuesdays, SAP Notes

3 SAP Leadership would take accountability provide the updates

4 Provides detailed and easy to find info about how they store their users' data

5 Gives the power back to the consumer by having them opt-out of sharing their data

Resources @ Finger Tips

Resources:

- [SAP Trust Center](#) Overview

- [The Trust Corner](#) Podcast

- [Security Community Content](#) and Blog

In the News:

- [Cybersecurity Month](#) (Dark Reading)

- [Leadership Podcast](#) hosted by General Stan McChrystal

Events:

- [CNBC Evolve Global Summit](#) (Video)

- Recognizing and Preventing Attacks on SAP S/4Hana (Upcoming Event, [Register Here](#))