**Subject:** Re: Quick
**Date:** Monday, 15 May 2017 at 19:01:00 Western European Summer Time
**From:** Ian Trump
**To:** [redacted]

Thank you,

You are a gentleman, Sir! I'll let you know.

Ian

Chief Technology Officer
[redacted]
👽

**From:** "[redacted]" [redacted]@solarwinds.com>
**Date:** Monday, May 15, 2017 at 18:49
**To:** Ian Trump [redacted]
**Subject:** RE: Quick

Ian,

Thanks for your note. I agree with our assessment and I appreciate the effort and candor you put behind trying to do the right thing at SolarWinds. I wish you the best in your new role and I sincerely hope it gives you the opportunity to do exactly what you wanted to do.

Let me know when you have your flights to Austin booked

Thanks

[redacted]

**From:** Ian Trump [[redacted]
**Sent:** Monday, May 15, 2017 10:54 AM
**To:** [redacted] <[redacted]@solarwinds.com>
**Subject:** Re: Quick

Hi [redacted],

Much appreciated. It saddens me greatly to leave but, the organisation was not interested in accommodating me or retaining my services at my level of expectation.

Often, one has to look outside to get to their next level of development. It's telling to me that my job and plan were essentially used for the VP architecture job which was posted prior to my departure. Yet I was not considered for the role.

My job at LogicNow was to increase the valuation of LogicNow by building a security brand out of an RMM tool. With few resources and minimal support I am immensely proud of that accomplishment. An accomplishment which is linked to my personal brand in the MSP and Security community.

Unfortunately and in my opinion the current SW MSP leadership is unable to support that brand and unwilling to make the corrections necessary. A point I made in my briefing to the CIO - a point perhaps I made too emphatically.

Whatever the case, when you have lost faith in the leadership and can't fix the problem you need to look else where to find your next thing that fulfils you.

For me that is not to watch a brand I built die and too effect positive change in an organisation. Too painful to be a part of, too painful to watch from the sidelines as mistake after mistake unfolded. All the same though, great life lessons and a illustrative story of "how not to SaaS" so many experiences (some great, some not so great) to take forward to my next job and the next one after that.

Truly wishing you all the best and I am sure are paths will cross again. I'll be presenting at channel con in Austin. Probably on state sponsored malware - talk about a topical conversation these days.

Ian

Sent from my iPhone

On 15 May 2017, at 16:22, [redacted] <[redacted]@solarwinds.com> wrote:

> Two more emails for you. I don't mind forwarding anything that comes to you that seems relevant
>
> I am sorry we did not get to say goodbye and to thanks you for everything you did. I hope we stay in touch. I texted you on the 11th without luck.
>
> Wish you all the best
>
> -[redacted]
>
> <mime-attachment>
>
> <mime-attachment>

# Creating Security

# The Corporate Security Plan (360 Days)

**Moving SolarWinds internally to a more robust security posture and changing the market perception of SolarWinds to a security brand will require resources, key personnel and organizational commitment. I believe significant progress and achievement can be realized within a year.**

Leadership for these deliverables is key:

1. Appoint a Sr. Director of Cyber Security, reporting to the CIO (Leadership)
2. Develop an Internal Security Messaging Plan (Prepare)
3. Create Functional Organization Security (Organize)
4. Develop a Commitment to Organizational Security (Execute)
5. Sustain Organizational Security (Sustain)

# The Internal Security Message Plan (90 Days)

1. Any company providing IT solutions & especially a company providing SaaS is already a security brand!

2. The distance between software tools that monitor and software tools that help secure is nuance:

Monitoring is Security!

As an IT solution provider we need to accept truths of the marketplace in which we exist:

- We need to live within the security brand
- We need to be good cyber security citizens
- Data breach is bad for us & bad for our customers
- Data breach of our company and customers is inevitable
- The capabilities of external protagonists are equally matched by internal mistakes or malicious activity

# The Internal Security Message (90 Days)

**Given these truths a corporate response is straightforward:**

- We will own, develop, test & execute a data breach plan to protect the corporation
- We will be ready for whatever comes our way: internal or external threat
- We will develop, own, & improve the security of our solutions to protect our customers
- We will benchmark our success, there is no “good” or “bad”, only better
- We will accept failure, but will be relentless in improving solution and corporate security
- The survival of the company depends on an internal commitment to security
- The survival of our customers depends on a commitment to build secure solutions
- The link between secure solutions and a secure company provides revenue and sustains the business

# The Internal Security Message (90 Days)

## A. Customer

- Paying me to care about their data
- I must secure and provide access to their data
- I  must watch their activity for signs of stupidity or malicious activity
- I must log their activity
- I  must keep my service up to date and secure from non-customers
- Customers make me $

## B. Non-Customer

- Not paying me to care about their data
- I must not provide access or let them degrade access
- They have no data on my system so I will not care about them
- I will not care about their politics, motivation or capabilities because they are not my customer
- They want to take my $

# Marketing Need (90 Days)

- Cybersecurity Market Reaches $75 Billion In 2015, expected to reach $170 Billion By 2020 (*Forbes*)
- Cyber Crime Costs Projected To Reach $2 Trillion by 2019 (*Forbes*)
- Internet value chain is expected to grow at 11 per cent per annum over the next five years, which will lead the total value of the internet value chain to grow from $3.5 trillion in 2015 to $5.8 trillion by 2020 (*GMSA/AT Kearney*)

# Marketing Impact (90 Days)

**The SolarWinds Security Story:**

**We are the only technology vendor who has a complete suite of security solutions for Protection, Detection & Recovery - for SMB, MSP and enterprise customers.**

- Immediate Go-to-Market Strategy required
- We don’t sell security products, we sell security solutions which provide visibility of organizational security compliance & security posture
- Combine all solutions into two security solution offerings: SaaS & on-premises
- All sales staff (MSP and SW Corp) should be able to sell any solution to any customer
- Remove SolarWinds MSP as a product brand name, call SaaS solutions “Cloud Services” or “Subscription Based Solutions”
- Redefined existing solutions: Network Management, becomes Network Security Management, etc.

# Strategic Impact (90 Days)

**Examination of existing solutions & future buy, build, license or partner options:**

**We are the only technology vendor who has a complete suite of security solutions for Protection, Detection & Recovery, for SMB, MSP and enterprise customers.**

[redacted]

[redacted]

# Strategic Concerns (90 Days)

**Examination of existing customer churn:**

- Fix the billing system, multiple bills for multiple solutions (not just MSP issue)
- Need a Professional Services Automation (PSA solution) to tie all SaaS and on-premises solutions into one reporting/billing/ticketing/dispatch system
- Monthly summary of service tickets opened, in progress and closed sent to customers
- Money is good, we should be able to take money any way that works for the customer: monthly, annually, automatic renewal, credit card, invoice, PayPal, etc.

**The fishing with a Dragnet problem:**

- Low touch or frictionless onboarding will yield far more non-MSP clients than MSP clients
- Non-MSP clients do not generally grow and are generally not interested in “grow your business” messaging
- Medium to large MSPs will not be sold to in this fashion
- MSPs are generally technical, the more non-MSP customers the greater support requirement

# Functional Organizational Security (180 Days)

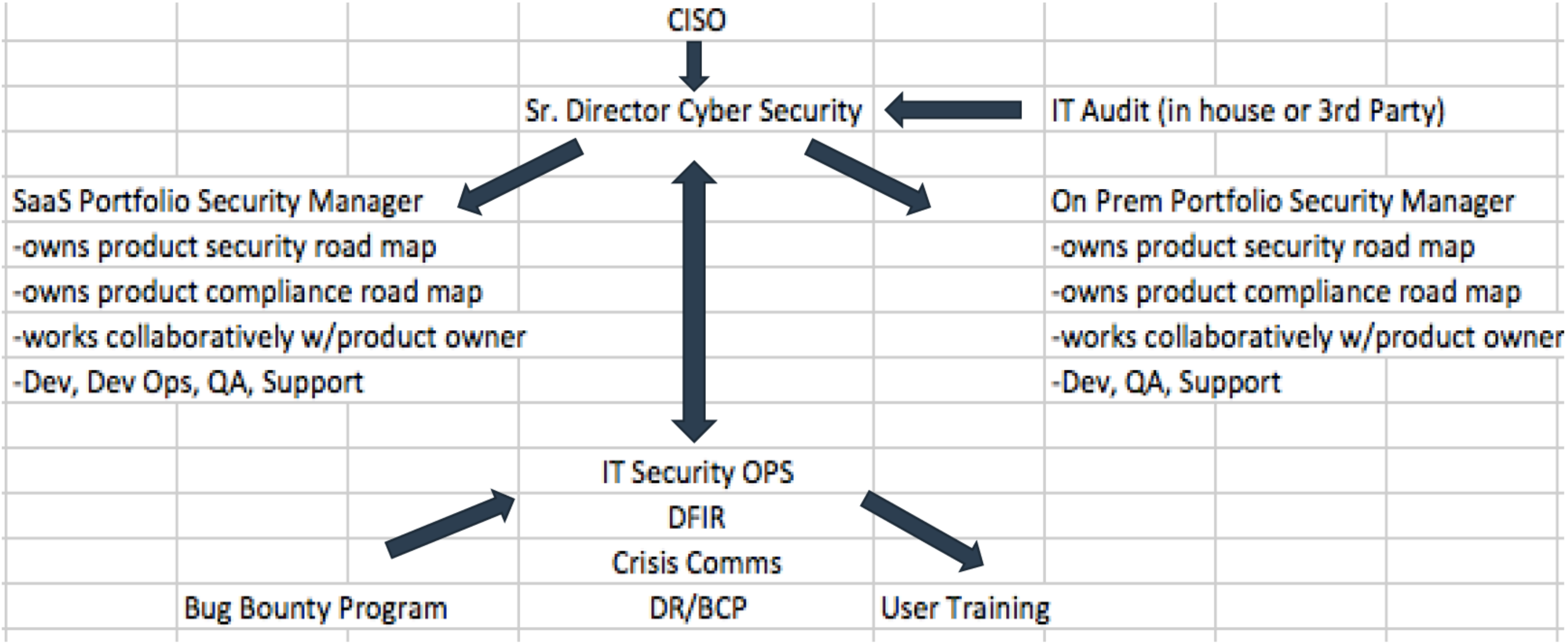
There are four functional areas of security:

1. Corporate Compliance
2. Corporate Security (includes 3rd Party Providers)
3. Solution Compliance
4. Solution Security (includes SaaS infrastructure)

Parts of these four functional areas exist today

- No centralized reporting
- No centralized management
- Silos of communication
- Duplication & redundant activity

# Functional Organizational Security (180 Days)



CISO

Sr. Director Cyber Security

IT Audit (in house or 3rd Party)

SaaS Portfolio Security Manager
-owns product security road map
-owns product compliance road map
-works collaboratively w/product owner
-Dev, Dev Ops, QA, Support

On Prem Portfolio Security Manager
-owns product security road map
-owns product compliance road map
-works collaboratively w/product owner
-Dev, QA, Support

IT Security OPS
DFIR
Crisis Comms
DR/BCP

Bug Bounty Program

User Training

# Functional Organizational Security (180 Days)

**In addition to the Sr. Director of Cyber Security (SDCS), two new positions: Portfolio Security Managers (PSM) are required to create and implement a security roadmap for solution compliance and solution security. As on-premises and SaaS solutions are diverse in nature it is prudent to separate the job responsibilities.**

- Note the input from 3rd party or internal IT audit directs the SDCS to provide guidance to PSM or IT Sec Ops as required
- Note the expansion of IT Sec Ops to receive bug bounty input & pen test information and send it to the SDCS for review and guidance to the appropriate PSM
- Note IT Sec OPS will own delivery of User Security Training (coordinating with HR)
- Note IT Sec OPS will have two-way communication to the SDCS providing direction to and receiving direction from.
- Note the expansion of IT Sec Ops to include DFIR, Crisis Coms (as per the Crisis communication plan) and DR/BCP
- IT Sec OPS and SDCS will provide business SLAs based on resources and capability

# Critical Role for the PSMs (180 Days)<-Starting Point

**Our security solutions, SaaS infrastructure and corporate systems exist in a precarious state – one moment we are secure and the next moment we are vulnerable. The recent Apache Struts vulnerability which cyber criminals quickly exploited caused brand damage and led to the compromise of over 500 customer systems – representing 10% of the install base of this solution.**

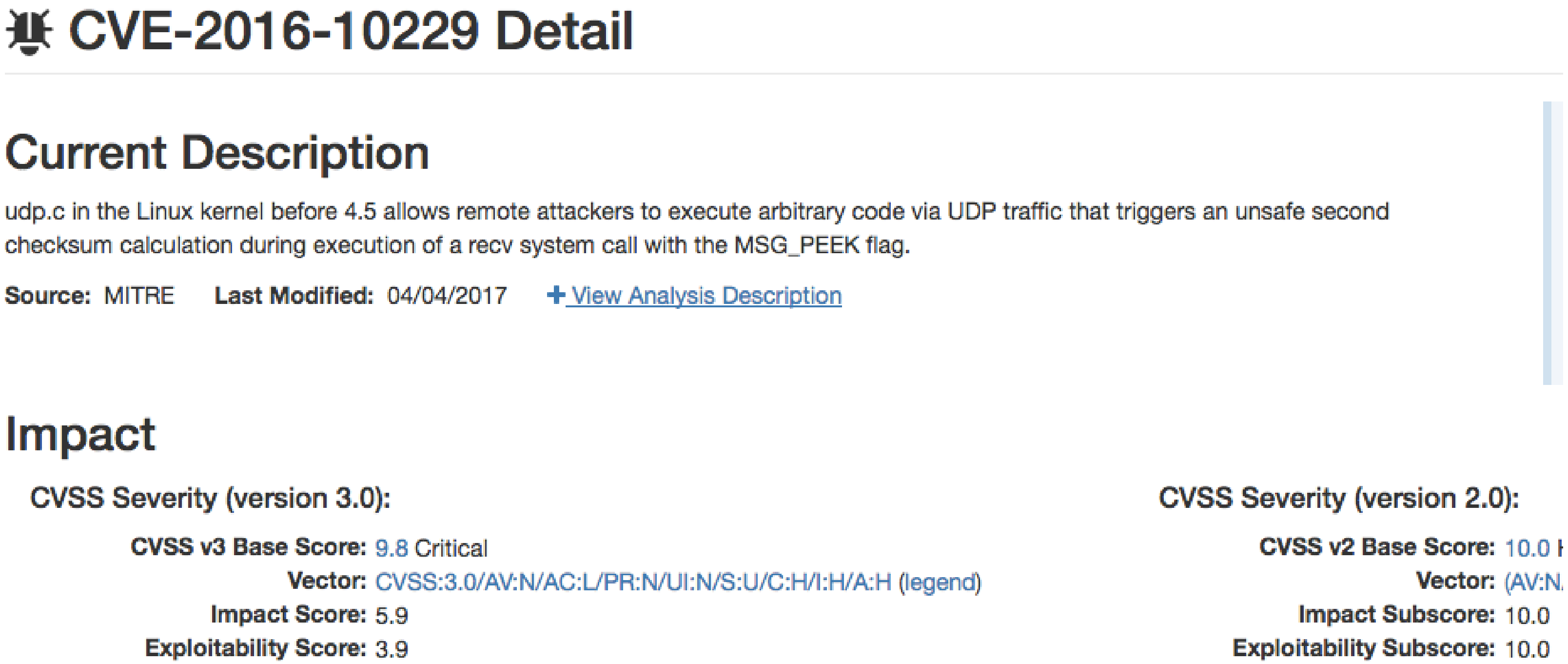
- PSM's must own the vulnerability monitoring (Full Disclosure, CERT and NVD) and remediation effort for security solutions in their portfolio

- PSM's working with the solution owner/manager, must become familiar with the dependencies required for each solution and advise when a vulnerability is published

- IT Sec Ops must own the vulnerability monitoring (Full Disclosure, CERT and NVD) and remediation efforts for the corporate infrastructure

**Vulnerability management is critical for secure solutions, secure infrastructure and secure corporate systems.**

# Critical Role for the PSMs (180 Days)



## CVE-2016-10229 Detail

### Current Description

udp.c in the Linux kernel before 4.5 allows remote attackers to execute arbitrary code via UDP traffic that triggers an unsafe second checksum calculation during execution of a recv system call with the MSG_PEEK flag.

**Source:** MITRE **Last Modified:** 04/04/2017 + View Analysis Description

### Impact

**CVSS Severity (version 3.0):**

**CVSS v3 Base Score:** 9.8 Critical
**Vector:** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H (legend)
**Impact Score:** 5.9
**Exploitability Score:** 3.9

**CVSS Severity (version 2.0):**

**CVSS v2 Base Score:** 10.0
**Vector:** (AV:N
**Impact Subscore:** 10.0
**Exploitability Subscore:** 10.0

**In the above example (recently raised on 4 Apr 17 to a 10/10 CVS 2.0 Score)**

- Who owns the documentation of our solutions, SaaS infrastructure & corporate system to determine if this is a severe vulnerability for our organization or our solutions?
- Who owns the responsibility to remediate the vulnerability of a solution, SaaS infrastructure or corporate system?

# Commitment to Organizational Security (90 Days)

***Gamification*** **is the process of taking something that already exists – our organization – and integrating game mechanics into it to motivate participation, engagement, and loyalty.**

- **Solution** – establish a program which provides “scoring” for moving compliance and/or security from “needs improvement” to “meets best practices” to “exceeds best practices”
- **Corporate** – establish a program which provides “scoring” for completing modules of security awareness (Business, Home, Travel, etc.), passing the modular tests and successfully applying best security practices against simulated corporate threats
- **IT Sec Ops** – establish 2 exercises per year – 1 table top walkthrough and a scenario based cyber incident to exercise response capabilities, learn from mistakes and identify knowledge gaps

# Commitment to Organizational Security - Example (90 Days)

[redacted]

[redacted]

[redacted]

Imagine if each of your employees saw themselves as defenders on a quest to protect their infrastructure.

[redacted] makes this reality through [redacted] Applied Fiction process. Employees will learn their roles and duties along with the reason why each duty is important – in their language.

The International Learning Technologies Awards for 2016 have been announced and [redacted] is winner of the “Best use of learning technologies to ensure compliance” category.

## Sustain Organizational Security (on going)

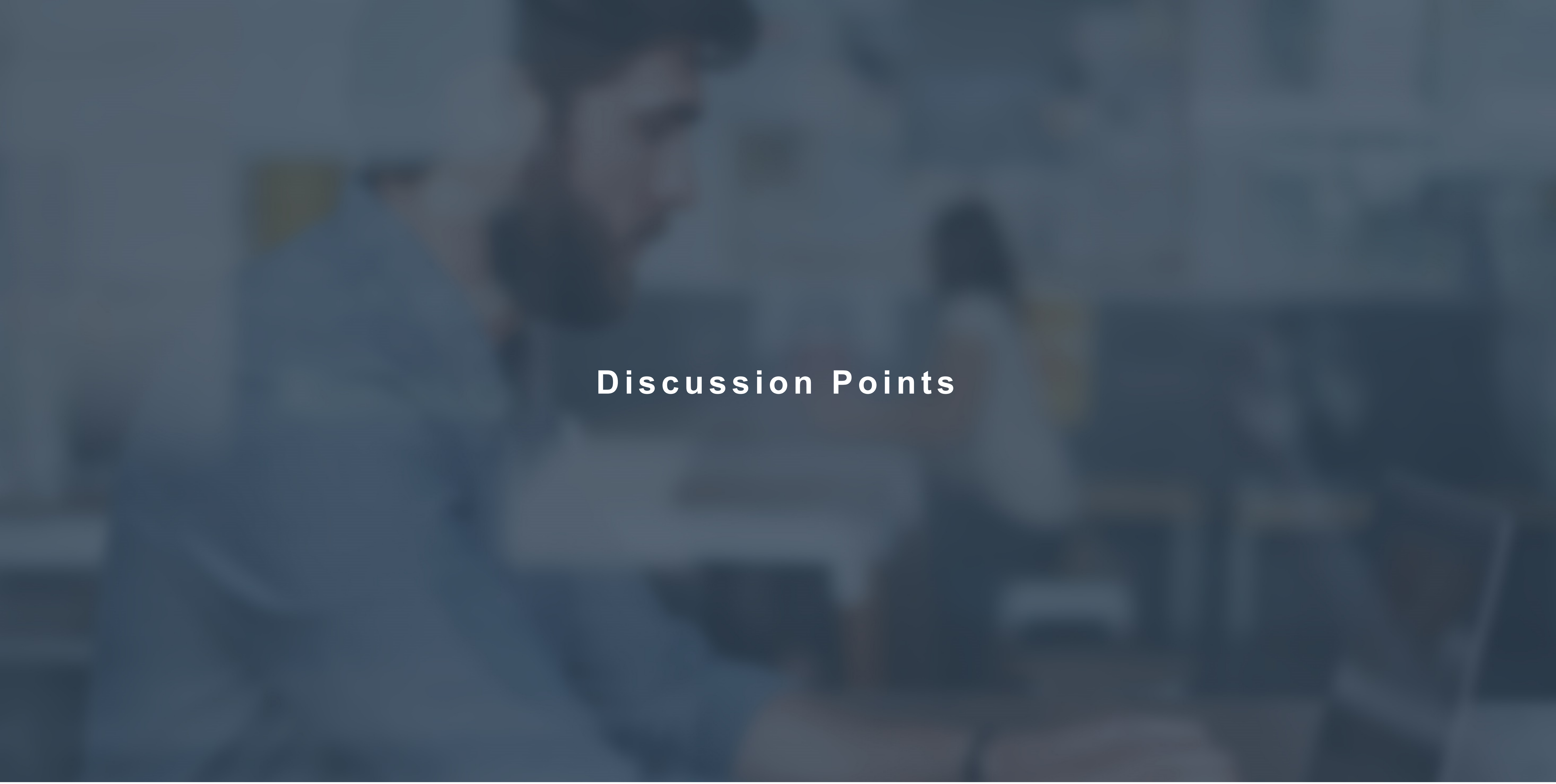
**Sustaining the culture of security once the resources, key personnel & organizational changes have been made is supported by principles of security leadership which messaging and functional security have established over the past year.**

**Continuing to message on the below topics will build, sustain and enhance corporate and solution security. These are:**

1. Achieve personal and professional security competence
2. Embrace personal and professional security improvement
3. Accept personal responsibility for security
4. Set a personal example of being secure
5. Ensure everyone knows the meaning and intent of security
6. Embrace security improvement opportunities
7. Make sound and timely security decisions
8. Never ignore a security incident, inform your supervisor and/or security operations

# SaaS & On-premises

- Corporation & 3rd Parties must be compliant and secure
- Solutions can not provide compliance, but they must not introduce non-compliant elements
- Our solutions are only as secure as our partners environments
    - More partner education on secure implementation, best practices & securing their business is required
- Solution security roadmaps need to be established
- We need to be transparent on the life cycle of solutions and create a succession plan for solutions
- If we can’t secure it, we should not advise partners to connect it without precautions and guidance



# Discussion Points

# GDPR in Brief

1. Increased fines - 4% of global turnover or €20,000,000
2. Opt-in consent - Clear, no opt-out, use data only as agreed
3. Breach notification - 72 hours to regulators, users “without delay”
4. Territorial scope - All organizations with data on EU individuals
5. Joint liability - Data controllers and processors
6. Right to removal - The users are in charge
7. Removes ambiguity - 28 laws become one
8. Data transfer - Data keeps privacy rights as it moves globally
9. Common enforcement - Authorities will be strict
10. Collective redress - Class action lawsuits from individuals

**Goes into effect 25 May 2018**

# GDPR Corporate Progress

Goal: By 1 May 18 - Ensure corporate security polices, corporate security procedures meet minimum data protection standards under the GDPR.

1. Conduct GDPR gap analysis on corporate security polices & corporate security procedures
2. Construct roadmap for to meet minimum data protection requirements under GDPR

Goal: By 1 May 18 – Ensure all SaaS solutions sold in EU/UK meet minimum data protection standards under GDPR

1. Conduct GDPR gap analysis on all SaaS solutions sold in EU/UK.
2. Construct roadmap to meet minimum data protection requirements under GDPR

# Partner GDPR Nervousness

**GDPR is a law as such compliance is mandatory and supervisory authorities powers are extensive and compliance with supervisory authority demands is compulsory.**

- Organizationally, we need to communicate our roadmap, report milestones and have a single point of contact (Data Privacy Officer)

- We need to ensure we have an IT-audit function established to provide ongoing gap analysis of our GDPR compliance posture

- We need to assure our customers we will be ready as an organization for GDPR
- We need to be responsive to their needs as partners, resellers and distributors

# Q&A