



Virginia Information Technologies Agency

Welcome and Opening Remarks

Mike Watson

January 8, 2019



ISOAG January Agenda

- **Welcome and Opening Remarks - Mike Watson, VITA**
- **Blind Spot Monitoring- Chris Atha, National White Collar Crime Center**
- **Advanced Persistent Security- Ira Winkler, Secure Mentem**
- **Cloud Readiness & Governance- Benjamin Sady, Dixon Hughes Goodman**



Chris Atha

No slides available

Advance Persistent Security

Ira Winkler, CISSP

ira@trustwave.com

+1-443-994-0245

January 2020





Why The Hype Matters to Us



It destroys our focus

It changes the story

It asks questions that shouldn't be asked

It deflects blame

Bad security vs unstoppable enemy

“If the top organizations can be hit, there is no way anyone will expect us to stop the attacks”

The Question That Should Be Asked



Was it really a “sophisticated” attack, or just bad security?



The Proclaimed “Sophisticated Attacks”



Sony

IRS

Ashley Madison

ISIS hacks

Healthcare companies

Retailers

You name it, it's sophisticated according to someone



It Can Also Help You



It gets people talking about security

Use the narrative to help your cause

If management is concerned about the hype, use it

Highlighting the common vulnerabilities exploited during attacks can get you funding to mitigate similar vulnerabilities

Stating how your security would have stopped the attacks would give you kudos

Hacking Team



Notable in that they supposedly support law enforcement and had zero day vulnerabilities

Embarrassing data to customers

Leak of vulnerabilities causing ripple effect



]HackingTeam[
]HackedTeam[

Sophisticated?



There was a Zero-day to get in

Password was passw0rd

Able to access and download data as engineer

Sophisticated: HELL NO!

Once inside there was apparently a flat network, easy data access, and no detection

IRS Breach



700,000 records compromised through Get Transcript function

X Million attempted breaches

Compromised authentication scheme

Required “information on the taxpayer had”

Criminal downloaded records, filed false tax returns

Stole \$50 Million

IRS Commissioner said it couldn't be stopped citing

Smart criminals with lots of advanced computers, hiring smart people



Sophisticated?



All the criminals needed were credit reports

IRS used commercial system that asked questions with answers available through credit reports

Went undetected for 700,000 relatively intensive attempts

Ashley Madison



Compromise of clients and client information

Led to suicides

Led to great embarrassment for others

Demonstrated that they did not delete accounts as promised

Released sensitive internal documents

Revealed that there weren't many real women on site

Sophisticated?



SQL injection attacks likely

Criminals claimed that network poorly segmented

Pass1234 was root password on all servers

Poor password encryption used

Data not deleted

Arrogance



CENTCOM/TV5Monde



The world was talking about how advanced ISIS was

The media questioned the security of US Government systems and classified data

Politicians were horrified and wanted answers

It was their Twitter feed

It was their YouTube feed

French politicians called it an attack against free speech



Anthem



80,000,000 health care records compromised

Largest breach of his type

Potentially perpetrated by China

Seemed to have signature of Deep Panda, and pandas are from China

A large number of people have government access

Sophisticated?



Watering hole attack suspected

Compromised administrator credentials

Undetected for nine months

Massive querying of data

Commonalities



Improperly segmented networks

Detection Deficit Disorder

Ignoring or looking at incidents in wrong places

Failure to white list

Not monitoring critical systems

Poor awareness

No multi-factor authentication

Phishing messages

Preventing the IRS Attack



Frankly authentication might not be feasible to strengthen

Better detection

IP analysis

Rapid increase in requests

Focus on misuse detection

The Irari Rules of Sophisticated Attacks



Must not actualize because of a Phishing message

Malware must have been undetectable

Passwords were not easily guessed

User awareness exploited with poor awareness program in place

Known vulnerabilities cannot have been exploited

Multifactor authentication in use on critical systems

Passwords were not hardcoded into the systems (or on TV)

Detection capability was in place and not ignored

Proper network segmentation in place

User accounts had minimum privileges

Yes, I Do Have to Say It



Yeah, Really



Advanced Persistent Threat or ADAPTIVE Persistent Threat?



They are Persistent

They are a Threat

But they are more adaptive than they are advanced

Advanced implies sophisticated

Sophisticated implies unstoppable

APT Assumes Failure



Actually, “successful” APT assumes failure

They assume there will be countermeasures in place

They assume there will be detection mechanisms

They know they need to be adaptive

They are proactive

“Be like water” – Bruce Lee

Empty your mind, be formless.
Shapeless, like water.
If you put water into a cup,
it becomes the cup.
You put water into a bottle
and it becomes the bottle.
You put it in a teapot,
it becomes the teapot.
Now, water can flow or
it can crash.

李小龍
Bruce Lee





“Persistence and focus will get you in”

Rob Joyce

Chief, NSA Tailored Access Office

Advanced Persistent Security



Fight APT with APS

Adaptive Persistent Security, but Advanced Persistent Security is a better buzz term

Security programs must be adaptive

Security programs must assume failure

Designed to presume failure

Extrusion prevention > Intrusion prevention



Risk Management Implies Failure is Acceptable

IRS hack demonstrates availability requires better detection, not security

It can be more cost effective

Security is about Risk Management not perfect prevention

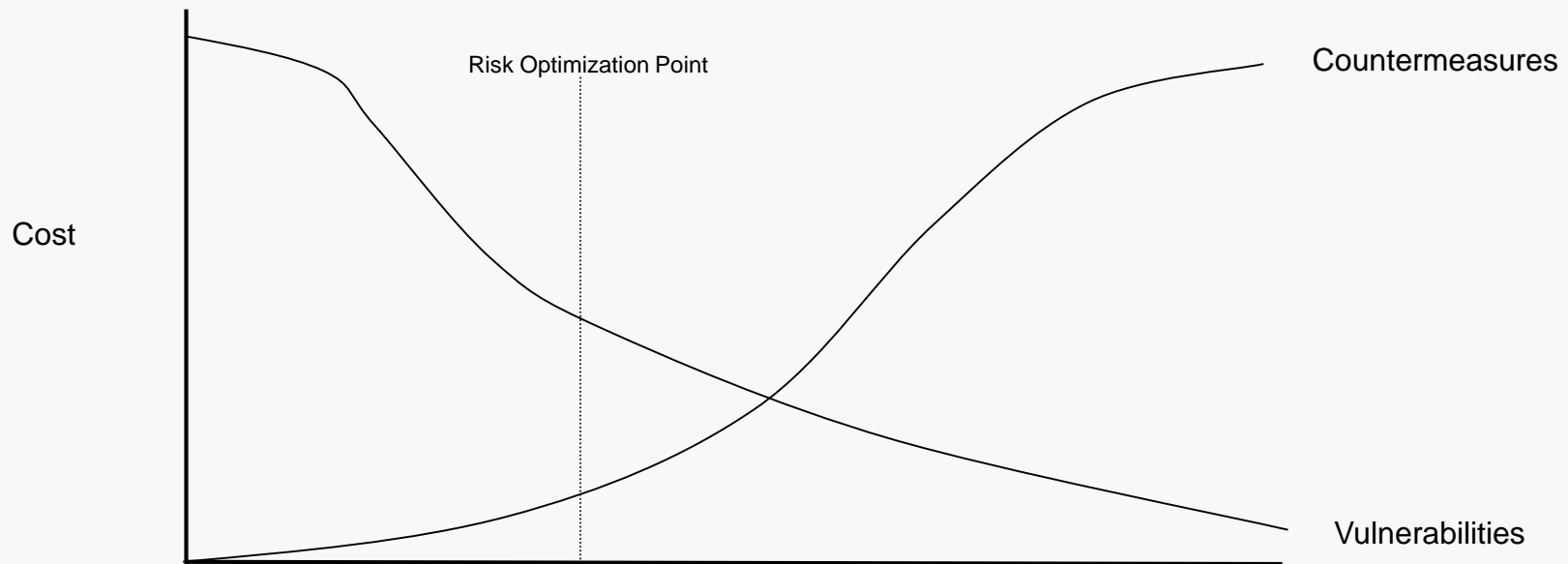
Detection and reaction mitigate loss that cannot be prevented

Adversary disruption is an acceptable “Security” strategy

Kill Chain Analysis

Goal is exit prevention

Optimizing Risk



Proaction



Design program always looking for failures

Determine where failure is likely to occur

Perform threat intelligence to determine likely attackers and attack vectors

Implement security countermeasures as appropriate

Implement detection

Build the ability to modify protection into your program

Defensive Information Warfare



Protection



Detection



Reaction



Protection



Understand what you Value

Understand your Threats

What they target

What they value

Likely attack vectors

Determine your vulnerabilities

Prioritize countermeasures based on likely threats and vulnerabilities

Address Security Culture

Detection



Understand your Kill Chain

Detection Deficit Disorder

Avoid it

Human sensors

Constantly examine the data

Assume critical assets are being stolen

Assume networks are compromised and look for indications



Reaction



Reaction should be anticipated as being a common circumstance

Reaction built into security program and architecture

Determine who's attacking you

What are their attack methods

Look for additional attacks

Be a hunter

Feedback into Protection

Remember, your goal is exit prevention

Extrusion prevention is more manageable intrusion prevention

The Role Security Culture/Awareness



People have a role in Prevention, Detection, and Reaction

A strong security culture prevents incidents

People should behave appropriately

A strong security culture detects incidents in progress

Snowden's coworkers should have noticed suspicious activity

Detecting incidents, phishing, etc.

Reaction

Reporting

Taking actions to mitigate incidents before they get too damaging



Conclusions



Attackers are successful not because they are advanced or sophisticated, but because they are adaptive and persistent

Be adaptive and persistent in response

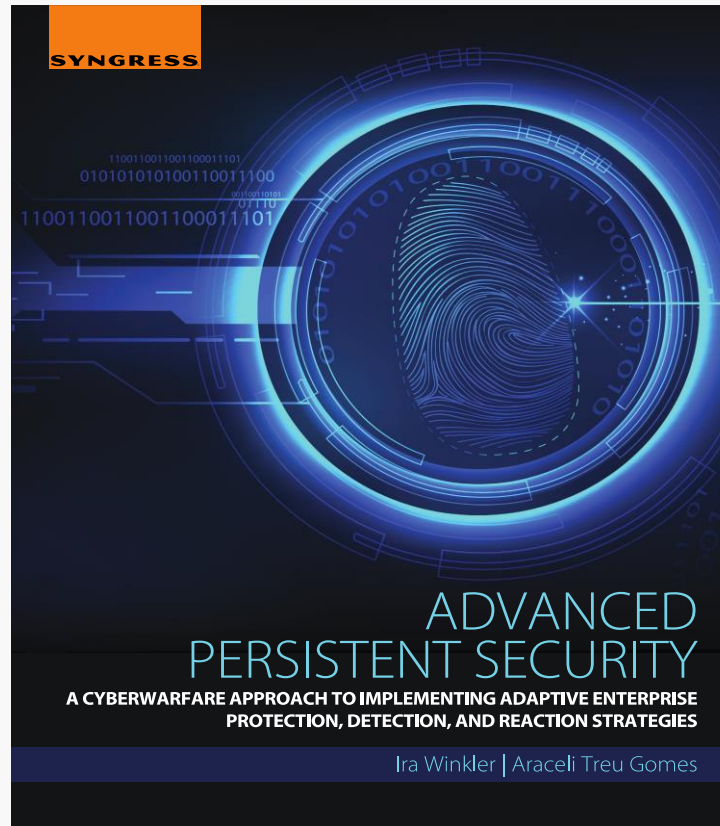
Be proactive

Failure is expected

Failure can be good

Implement Advanced Persistent Security

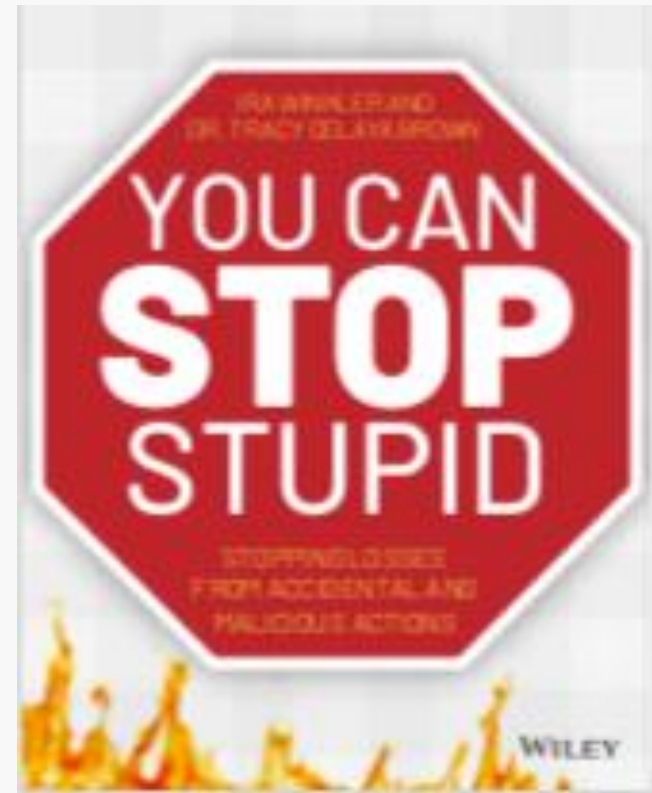
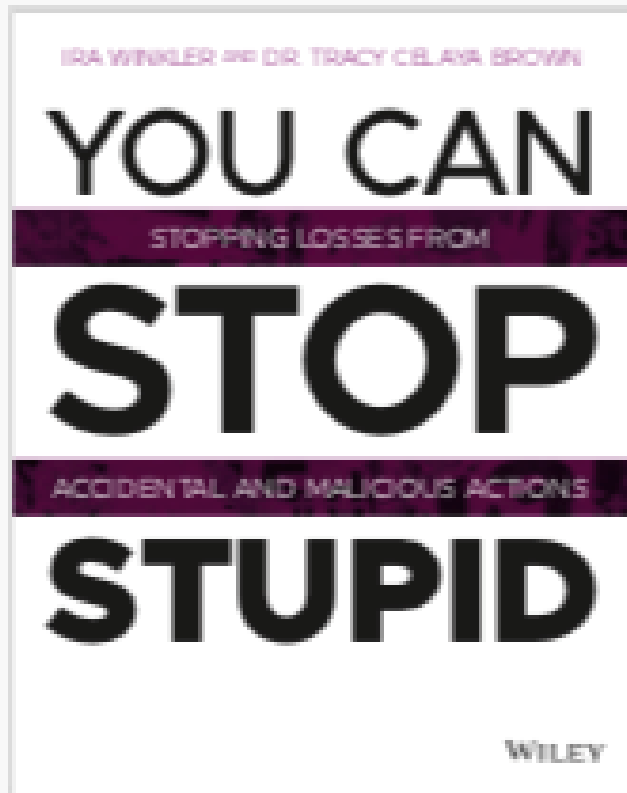
The Book, The Myth, The Legend





The Next Legend?

Which would you choose?



For More Information



ira@trustwave.com

+1-443-603-0200

[@irawinkler](#)

www.trustwave.com

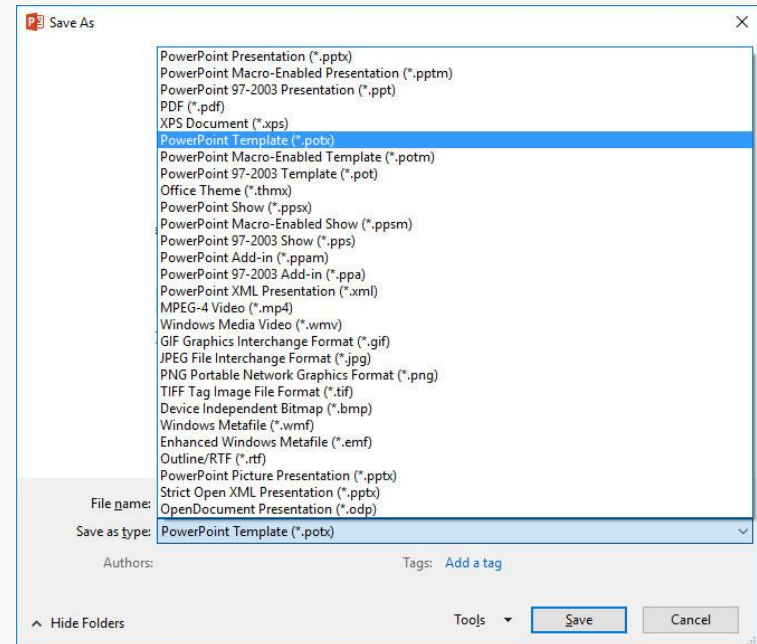
www.linkedin.com/in/irawinkler

Facebook.com/irawinkler

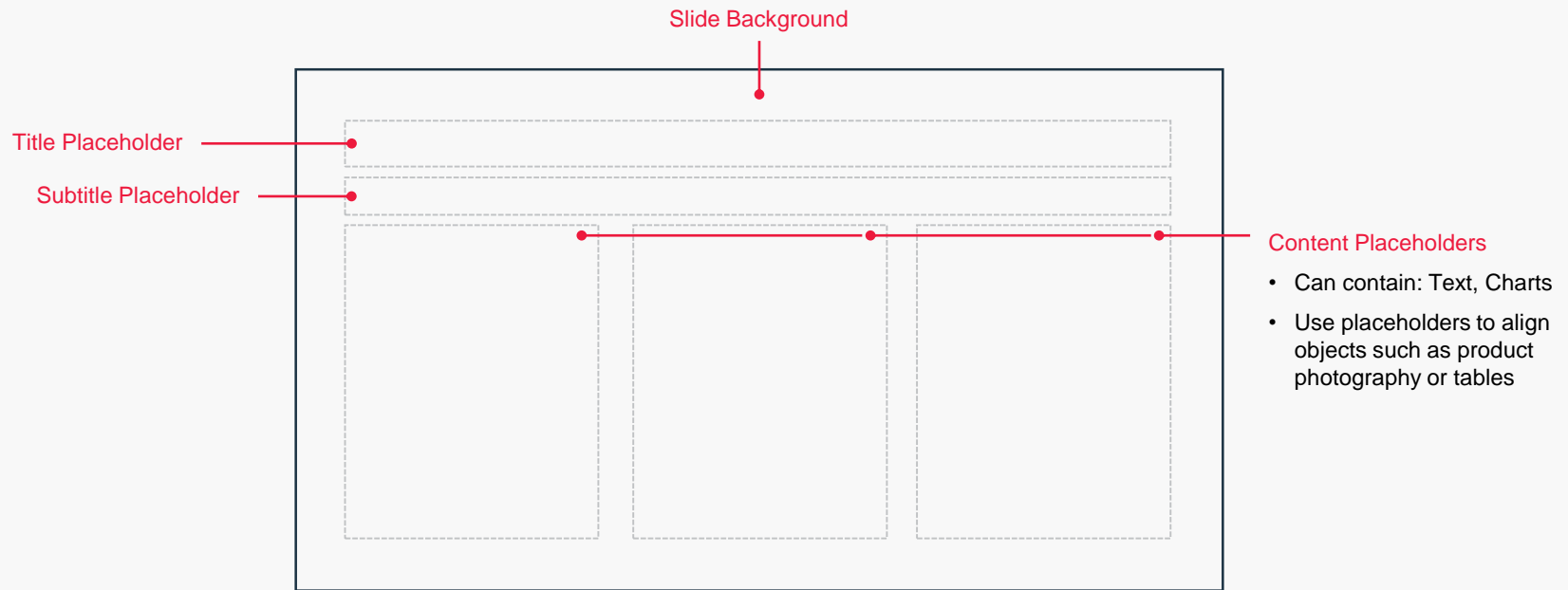
How to Save as Template



1. On the **File** tab, click **Save As**.
2. Under **Save**, click **Browse**.
3. In the **Save As** dialog box, in the File name box, type a file name for your template, or do nothing to accept the suggested file name.
4. In the Save as type list, choose PowerPoint Template (*.potx), and then select Save.
 - PowerPoint automatically stores your new template in the Custom Office Templates folder.
5. To use your template for a new presentation, click File > New.
 - In PowerPoint 2016, click Custom > Custom Office Templates, and then double-click the template you saved.
 - In PowerPoint 2013, click Personal, and then double-click the template you saved.



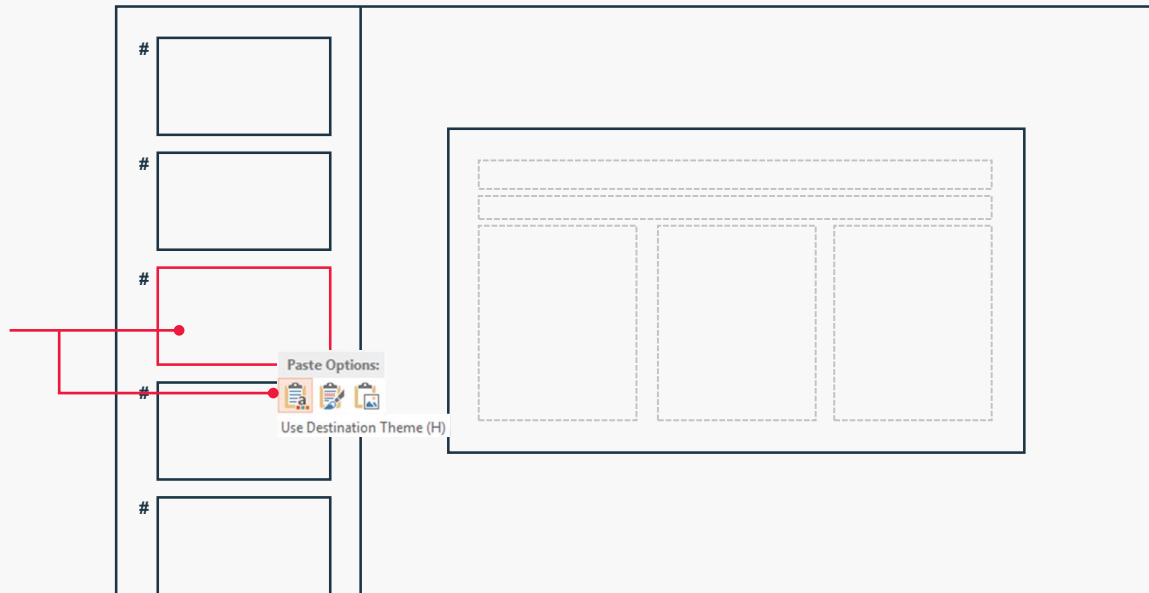
Slide Layout Anatomy



Adding Slides From Other Presentations



When you copy and paste slides from other presentations into this presentation, select **Use Destination Theme**



Type Styling



Headlines are capitalized based on AP rules using this tool.

<http://titlecapitalization.com/>

Sub-headlines are capitalized using sentence case.

First word is capitalized as you would a sentence, but all other words adhere to normal sentence capitalization standards.

Formatting Text



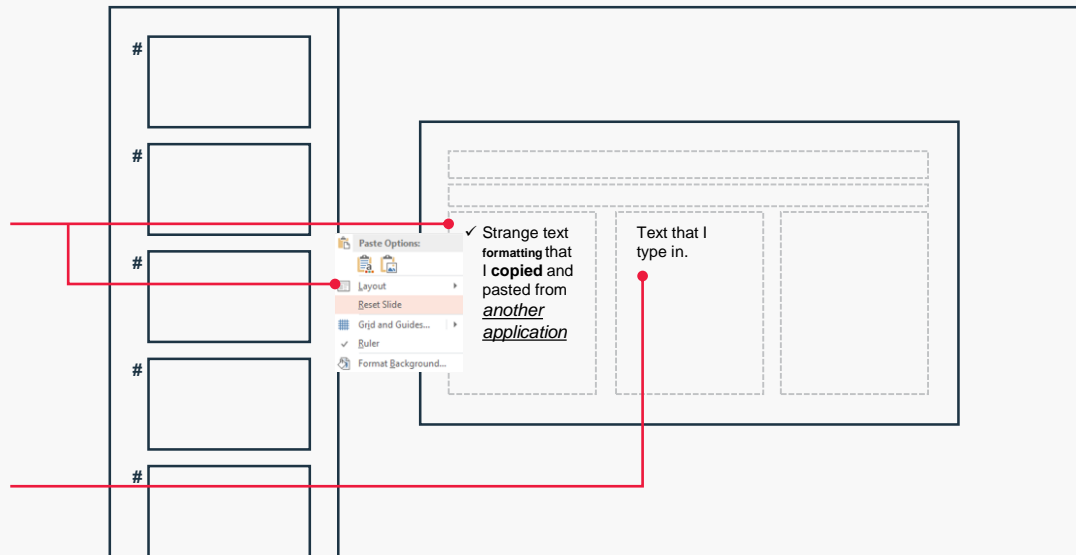
Adding text to your slide

When you copy and paste text from other presentations or applications, sometimes the formatting is inaccurate.

When this occurs, right-click the slide and select **Reset Slide** to default to the master format.

When your slide has been defaulted to the master layout or you type in your own text, use your **Tab Key** to adjust the text formatting.

See next slide for more info.



Formatting Text



Using Tabs to create bulleted text

PowerPoint has 9 bullet levels

These can be navigated by:

- Demote (down a level) by **pressing TAB**
- Promote (up a level) by **pressing SHIFT + TAB**

Bullet levels can be mixed and matched based on your content need

There is also a slide layout option for a larger Fourth Level named - Large bullet

Standard
bullet levels
Primary light content

Secondary
bullet levels
Specialty /
dense content

1 **Edit Master text styles: heading**

2 Second level: primary bullet

3 • Third level: primary bullet two

4 – Fourth level : secondary bullet

5 **large stats**

6 **Sixth Level: Stat Callout**

7 **secondary heading**

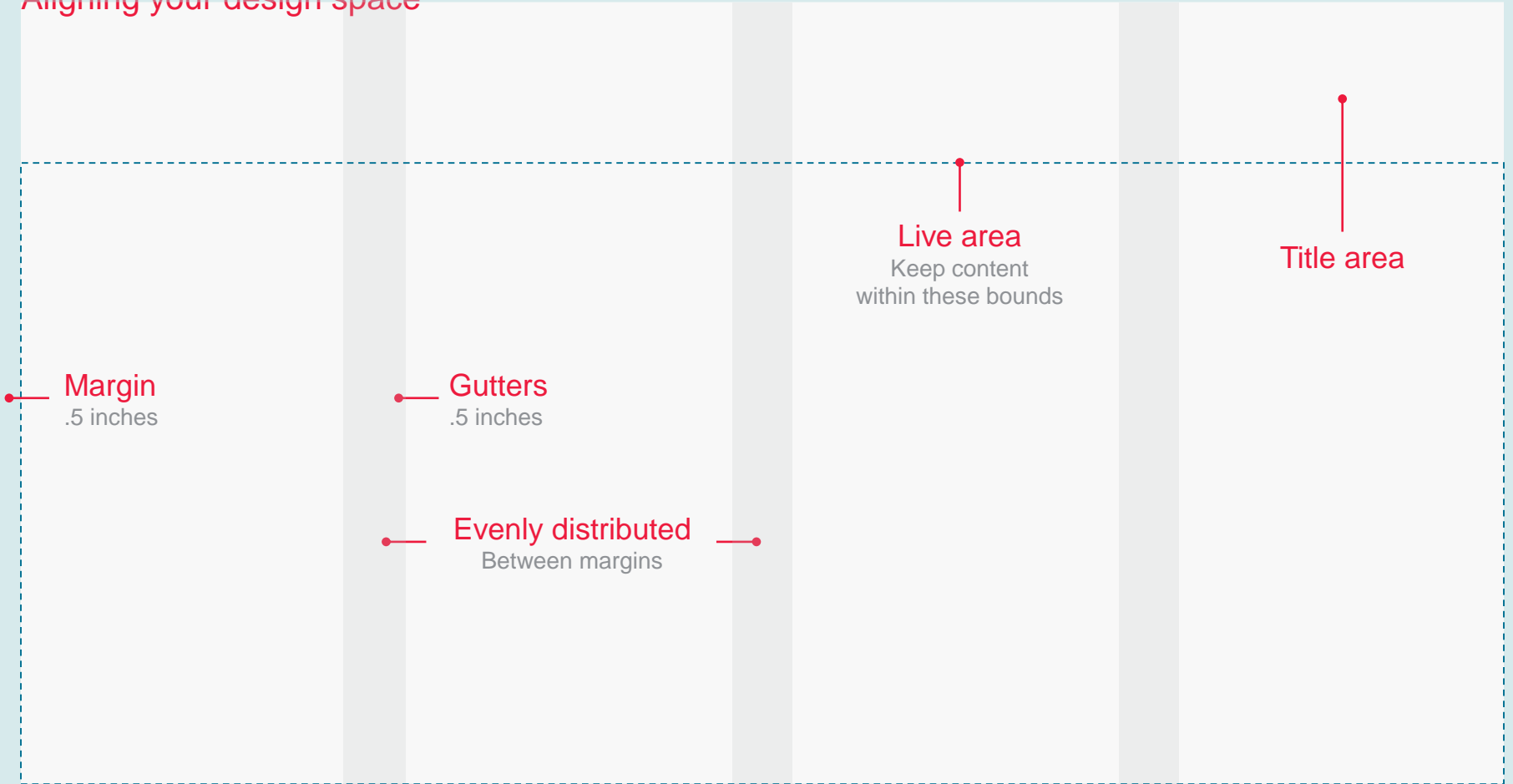
8 secondary subheading

9 • secondary bullet body

Grid Example



Aligning your design space



Photos



Use freely from approved library

The approved photos can be found on the Trustwave shared drive at “Photo Library”

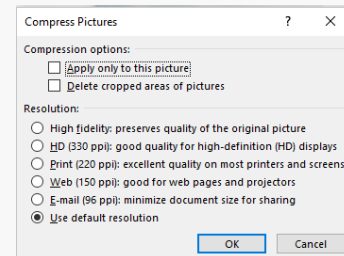
If you can't find what you need, please visit istockphoto.com and email marketing@trustwave.com with the exact photo.

- Marketing will decide if it meets guidelines and can be purchased
- We cannot provide same day purchases of photos

Only photos approved by marketing can be used

After final saving of your presentation, please compress the pictures

- To compress all pictures in your presentation, select any picture you added and go to Format > Compress Pictures.
- Choose the appropriate Resolution option from the following choices:



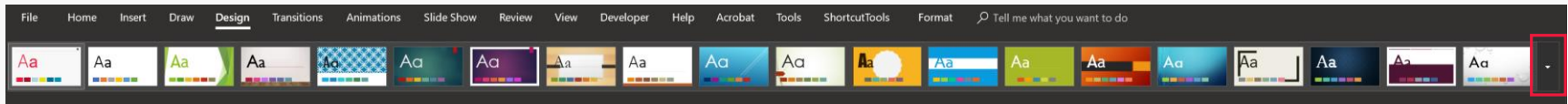
- Deselect “Apply only” and “Delete cropped”
- Click OK

Setting Your Default Theme



Important first step for migrating existing presentations

1. Launch PowerPoint
2. Use **File> New from Template**
3. Select the *new Trustwave template* to create a new presentation
4. Go to the **Design tab**
5. Expand the Themes Gallery
6. Select the **Save Current Theme** command
7. Name the Theme file **2018 Trustwave Corporate Template** & click **Save**
8. In the Themes Gallery, *right-click* the thumbnail named 2018 Trustwave Template & select **Set as Default Theme**



Click here to expand

Migrating Existing Presentations



Easy to do but be mindful of formatting

*****Follow the instructions from the previous slide first*****

Open the existing presentation in PowerPoint

Go to the **Design Tab**

Find the theme titled 2018 Trustwave Corporate Template (hover over each theme to see the name), *right-click* and choose **Apply to All Slides**

From the **Design Tab**, select *Slide Size* (right side of ribbon) and choose **Widescreen (16:9)**

For each slide in the existing presentation (now in widescreen format), *right-click* > **Layout** and choose the appropriate slide layout (*Title and Content* for most slides)

You will notice some changes that can only be fixed manually

All text must use the new template text boxes for consistent formatting

- One option is to copy text to Notepad (or your favorite text editor) and then copy back in to the presentation

Selecting and Editing Images



Working with existing images

Follow the instructions from the previous slide first

Pay close attention to existing images. The new template has a very light grey background and your existing images may have a white background. **Do not use images with a white background.**

- PNG images have transparent backgrounds and are the best choice
- When searching add PNG to the search
- To remove the colored background from an existing image
 - Double-click the picture, and when **Picture Tools** appears, click **Picture Tools Format > Remove Background**



- Select the areas you want transparent by highlighting with the purple marker

Master Layout Examples

Title Layout

SUBTITLE EXAMPLE

Name (first & last) placeholder

Position placeholder

January 8, 2020



Agenda Slide



01 Agenda Main Topic

02 Subtopic One

03 Subtopic Two

04 Subtopic Three

05 Subtopic Four

06 Agenda Main Topic

07 Subtopic One

08 Subtopic Two

09 Subtopic Three

10 Agenda Main Topic

11 Subtopic One

12 Subtopic Two

13 Subtopic Three

14 Subtopic Four

15 Agenda Main Topic

16 Subtopic One

17 Subtopic Two

18 Subtopic Three

Segue Slide Option

Segue Slide Option

Segue Slide Option

Title and Content Layout



Lorem ipsum dolor sit amet

Lorem ipsum dolor sit amet, consectetur adipiscing elit

Ut gravida nulla at tortor efficitur, sit amet mattis arcu convallis

- Etiam ornare est molestie, interdum ipsum volutpat, feugiat lacus

Lorem ipsum dolor sit amet, consectetur adipiscing elit

Ut gravida nulla at tortor efficitur, sit amet mattis arcu convallis

- Etiam ornare est molestie, interdum ipsum volutpat, feugiat lacus

Two Content Layout



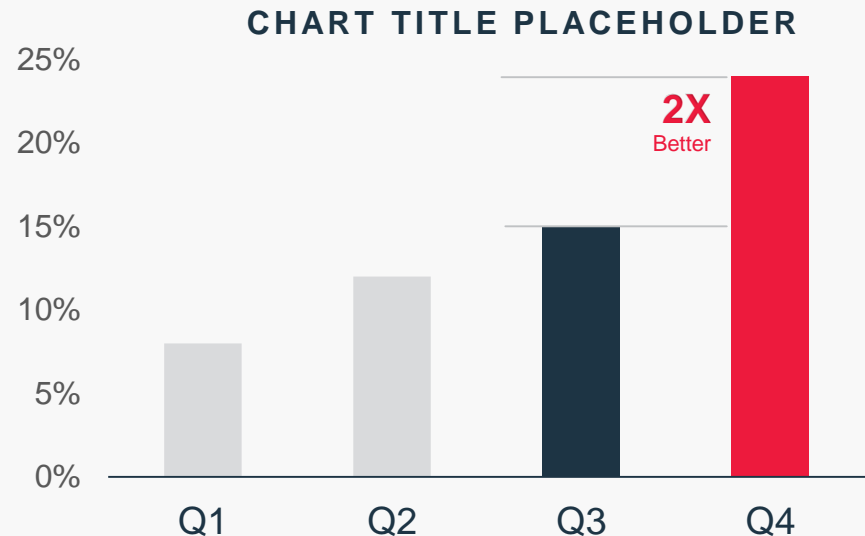
Lorem ipsum dolor sit amet, consectetur Ut gravida nulla

Main Point Goes here

Lorem ipsum dolor sit amet, consectetur Ut gravida nulla at tortor efficitur, sit amet mattis arcu convallis Etiam ornare est molestie, interdum ipsum volutpat, feugiat lacus

Main Point Goes here

Lorem ipsum dolor sit amet, consectetur Ut gravida nulla at tortor efficitur, sit amet mattis arcu convallis Etiam ornare est molestie, interdum ipsum volutpat, feugiat lacus



Two Content Layout



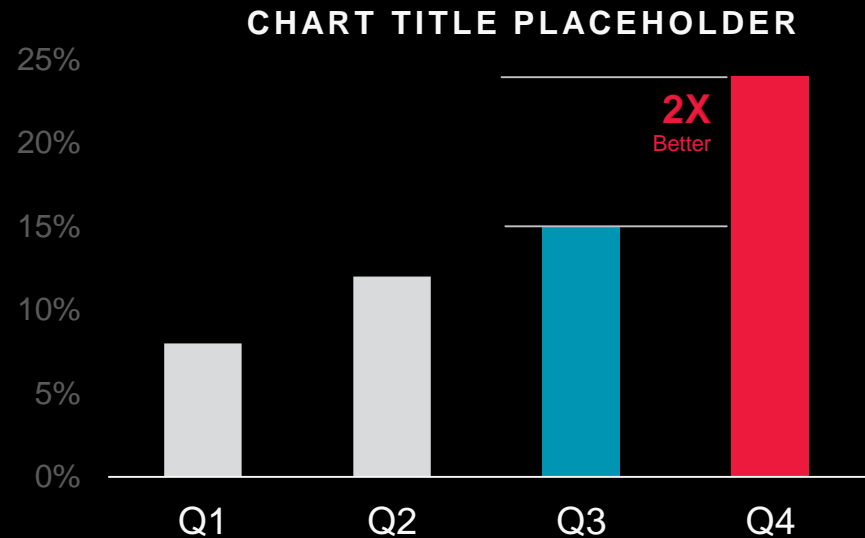
Lorem ipsum dolor sit amet, consectetur Ut gravida nulla

Main Point Goes here

Lorem ipsum dolor sit amet, consectetur Ut gravida nulla at tortor efficitur, sit amet mattis arcu convallis Etiam ornare est molestie, interdum ipsum volutpat, feugiat lacus

Main Point Goes here

Lorem ipsum dolor sit amet, consectetur Ut gravida nulla at tortor efficitur, sit amet mattis arcu convallis Etiam ornare est molestie, interdum ipsum volutpat, feugiat lacus



Two Content Call-Out



Main Point Goes here

Lorem ipsum dolor sit amet, consectetur Ut gravida nulla at tortor efficitur, sit amet mattis arcu convallis Etiam ornare est molestie, interdum ipsum volutpat, feugiat lacus

Main Point Goes here

Lorem ipsum dolor sit amet, consectetur Ut gravida nulla at tortor efficitur, sit amet mattis arcu convallis Etiam ornare est molestie, interdum ipsum volutpat, feugiat lacus

Main Point Goes Here.

Did you have a question?

Lorem ipsum dolor sit amet Ut gravida nulla at tortor efficitur, sit amet mattis arcu convallis Etiam ornare est molestie, interdum ipsum volutpat, feugiat lacus Ut gravida nulla at tortor efficitur, sit amet mattis arcu convallis Etiam ornare est molestie, interdum ipsum volutpat, feugiat lacus

Three Content Layout



Lorem ipsum dolor sit amet

**Lorem ipsum dolor sit amet Ut
gravida nulla at tortor efficitur, sit
amet mattis arcu convallis Etiam
ornare est molestie, interdum
ipsum volutpat, feugiat lacus**

Ut gravida nulla at tortor efficitur, sit amet
mattis arcu convallis

Lorem ipsum dolor sit amet

Ut gravida nulla at tortor efficitur,
sit amet mattis arcu convallis

- Etiam ornare est molestie, interdum
ipsum volutpat, feugiat lacus

Ut gravida nulla at tortor efficitur,
sit amet mattis arcu convallis

- Etiam ornare est molestie, interdum
ipsum volutpat, feugiat lacus

Lorem ipsum dolor sit amet

Ut gravida nulla at tortor efficitur,
sit amet mattis arcu convallis

- Etiam ornare est molestie, interdum
ipsum volutpat, feugiat lacus

Ut gravida nulla at tortor efficitur,
sit amet mattis arcu convallis

- Etiam ornare est molestie, interdum
ipsum volutpat, feugiat lacus

Four Content Layout



Lorem ipsum dolor sit amet

Lorem ipsum dolor sit amet Ut gravida nulla at tortor efficitur, sit amet mattis arcu convallis Etiam ornare est molestie, interdum

Ut gravida nulla at tortor efficitur, sit amet mattis arcu convallis

Lorem ipsum dolor sit

Ut gravida nulla at tortor efficitur, sit amet mattis arcu convallis Etiam ornare est molestie, interdum ipsum volutpat, feugiat

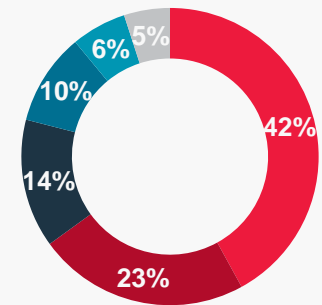
- Ut gravida nulla at tortor efficitur
- sit amet mattis arcu convallis

Lorem ipsum dolor sit

Ut gravida nulla at tortor efficitur, sit amet mattis arcu convallis Etiam ornare est molestie, interdum ipsum volutpat, feugiat

- Ut gravida nulla at tortor efficitur
- sit amet mattis arcu convallis

CHART TITLE



Title with Subtitle

Optional subtitle placeholder





Blank / Custom Layout



Image with Caption Right:

Lorem ipsum dolor sit amet,
consetur adipiscing elit ut
gravida nulla

Point one here

Lorem ipsum dolor sit amet, consetur
adipiscing elit ut gravida nulla

Point Two Here

Lorem ipsum dolor sit amet, consetur
adipiscing elit ut gravida nulla

Image with Caption Left:

Lorem ipsum dolor sit amet,
consetur adipiscing elit ut
gravida nulla

Point one here

Lorem ipsum dolor sit amet, consetur
adipiscing elit ut gravida nulla

Point Two Here

Lorem ipsum dolor sit amet, consetur
adipiscing elit ut gravida nulla





Image with Caption Right:

Lorem ipsum dolor sit amet, consetur adipiscing elit ut gravida nulla

Point one here

Lorem ipsum dolor sit amet, consetur adipiscing elit ut gravida nulla

Point Two Here

Lorem ipsum dolor sit amet, consetur adipiscing elit ut gravida nulla

Image with Caption Left:

Lorem ipsum dolor sit amet, consetur adipiscing elit ut gravida nulla

Point one here

Lorem ipsum dolor sit amet, consetur adipiscing elit ut gravida nulla

Point Two Here

Lorem ipsum dolor sit amet, consetur adipiscing elit ut gravida nulla





Image with Caption Right:

Lorem ipsum dolor sit amet, consetur adipiscing elit ut gravida nulla

Point one here

Lorem ipsum dolor sit amet, consetur adipiscing elit ut gravida nulla

Point Two Here

Lorem ipsum dolor sit amet, consetur adipiscing elit ut gravida nulla

Image with Caption Left:

Lorem ipsum dolor sit amet,
consetur adipiscing elit ut
gravida nulla

Point one here

Lorem ipsum dolor sit amet, consetur
adipiscing elit ut gravida nulla

Point Two Here

Lorem ipsum dolor sit amet, consetur
adipiscing elit ut gravida nulla





Image with Caption Right:

Lorem ipsum dolor sit amet, consetur adipiscing elit ut gravida nulla

Point one here

Lorem ipsum dolor sit amet, consetur adipiscing elit ut gravida nulla

Point Two Here

Lorem ipsum dolor sit amet, consetur adipiscing elit ut gravida nulla

Image with Caption Left:

Lorem ipsum dolor sit amet,
consetur adipiscing elit ut
gravida nulla

Point one here

Lorem ipsum dolor sit amet, consetur
adipiscing elit ut gravida nulla

Point Two Here

Lorem ipsum dolor sit amet, consetur
adipiscing elit ut gravida nulla



Six Stats Layout



\$100M

Lorem ipsum dolor

\$100M

Lorem ipsum dolor

\$100M

Lorem ipsum dolor

\$100M

Lorem ipsum dolor

\$100M

Lorem ipsum dolor

\$100M

Lorem ipsum dolor

Three Stats Layout



\$100M

Lorem ipsum dolor

\$100M

Lorem ipsum dolor

\$100M

Lorem ipsum dolor

Map Layout



Optional subtitle





“ Quote Layout: Lorem ipsum dolor sit amet, consectetur adipiscing elit Ut gravida nulla at tortor efficitur, sit amet mattis arcu convallis.

Name, Title, Source



“ **Quote Layout:** Lorem ipsum dolor sit amet, consectetur adipiscing elit Ut gravida nulla at tortor efficitur, sit amet mattis arcu convallis.

Quote Source | Date



Big Statement Layout: Lorem ipsum dolor sit amet, consectetur



Large statement goes
right here.

Challenges Layout

Lorem ipsum dolor sit amet, consetur
adipiscing elit ut gravida nulla

Point one here

Lorem ipsum dolor sit amet, consetur
adipiscing elit ut gravida nulla

Point Two Here

Lorem ipsum dolor sit amet, consetur
adipiscing elit ut gravida nulla



- 1 Challenge
- 2 Challenge
- 3 Challenge
- 4 Challenge
- 5 Challenge

Challenges Layout

Lorem ipsum dolor sit amet, consetur
adipiscing elit ut gravida nulla

Point one here

Lorem ipsum dolor sit amet, consetur
adipiscing elit ut gravida nulla

Point Two Here

Lorem ipsum dolor sit amet, consetur
adipiscing elit ut gravida nulla



- 1 Challenge
- 2 Challenge
- 3 Challenge
- 4 Challenge
- 5 Challenge

Challenges Layout

Lorem ipsum dolor sit amet, consetur
adipiscing elit ut gravida nulla

Point one here

Lorem ipsum dolor sit amet, consetur
adipiscing elit ut gravida nulla

Point Two Here

Lorem ipsum dolor sit amet, consetur
adipiscing elit ut gravida nulla



- 1 Challenge
- 2 Challenge
- 3 Challenge
- 4 Challenge
- 5 Challenge

Two Challenges Layout



Challenge Category 1

Challenge 1: High-level point

- Detailed point
- Detailed point
- Detailed point

Challenge 2: Placeholder text

- Detailed point
- Detailed point

Challenge 3: Placeholder text

- Detailed point

Challenge Category 2

Challenge 1: High-level point

- Detailed point
- Detailed point
- Detailed point

Challenge 2: Placeholder text

- Detailed point
- Detailed point

Challenge 3: Placeholder text

- Detailed point

Three Challenges Layout



Challenge Category 1

Challenge 1: High-level point

- Detailed point

Challenge 2: Placeholder text

- Detailed point

Challenge 3: Placeholder text

- Detailed point

Challenge Category 2

Challenge 1: High-level point

- Detailed point

Challenge 2: Placeholder text

- Detailed point

Challenge 3: Placeholder text

- Detailed point

Challenge Category 3

Challenge 1: High-level point

- Detailed point

Challenge 2: Placeholder text

- Detailed point

Challenge 3: Placeholder text

- Detailed point

Four Challenges Layout



Challenge Category 1

Challenge 1:
High-level point

- Detailed point

Challenge 2:
Placeholder text

- Detailed point

Challenge 3:
Placeholder text

- Detailed point

Challenge Category 2

Challenge 1:
High-level point

- Detailed point

Challenge 2:
Placeholder text

- Detailed point

Challenge 3:
Placeholder text

- Detailed point

Challenge Category 3

Challenge 1:
High-level point

- Detailed point

Challenge 2:
Placeholder text

- Detailed point

Challenge 3:
Placeholder text

- Detailed point

Challenge Category 4

Challenge 1:
High-level point

- Detailed point

Challenge 2:
Placeholder text

- Detailed point

Challenge 3:
Placeholder text

- Detailed point

Market Sector

The Challenges:

- Moving from Do-it-Yourself Security to Managed Security
- Additional protection against application vulnerabilities
- Threat analysis and advanced malware detection

The Solution:

Threat Management:

- Trustwave Log Management of security devices
- Managed SIEM and Threat Analysis to discover emerging threats

Vulnerability Management:

- Managed WAF across all internal and external web applications to insure protected data from outsider attacks

The Results

Correction of previous compliance issues

24x7x365 monitoring of log data and security events

Secure and compliant web applications for self-service customers





1/3 Photo with Text.

Title Can Go to 2 Lines

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Point one here

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Point Two Here

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.



Threat Report Layout

Threat:

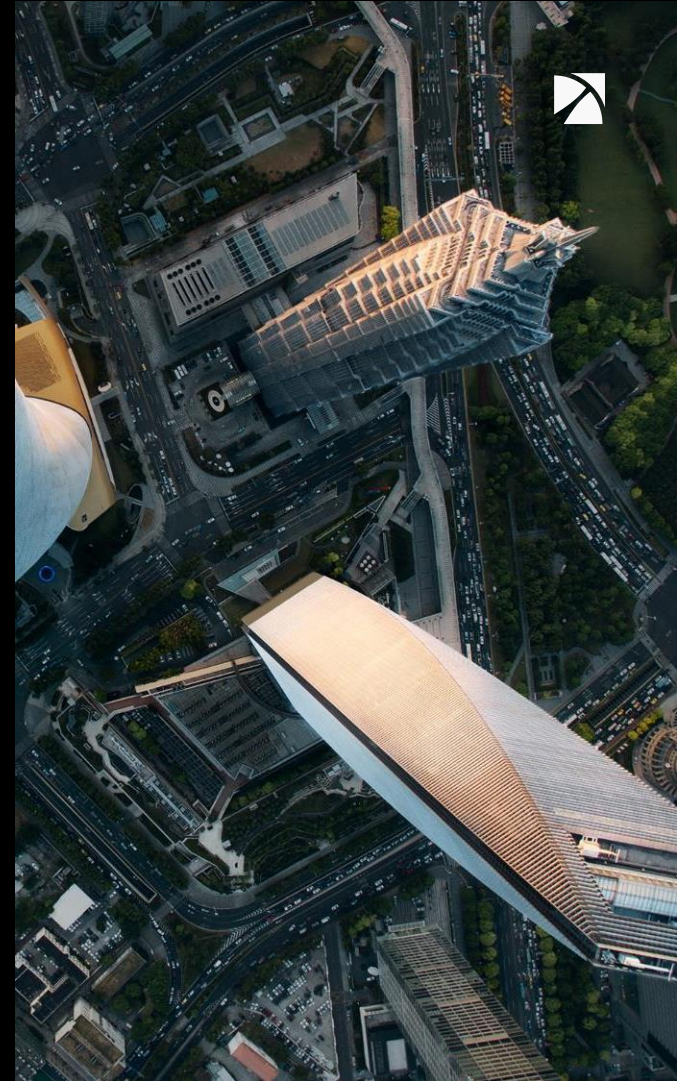
Lorem ipsum dolor sit amet, consectetur adipiscing elit.
Ut gravida nulla at tortor efficitur, sit amet mattis arcu

Discovery:

Lorem ipsum dolor sit amet, consectetur adipiscing elit.
Ut gravida nulla at tortor efficitur, sit amet mattis arcu

Recommendation:

Lorem ipsum dolor sit amet, consectetur adipiscing elit.
Ut gravida nulla at tortor efficitur, sit amet mattis arcu





Questions and Next Steps













Graphic Elements

Colors



Template theme colors w/ RGB values




Soft White	Black	Trustwave Red	Dark Slate	Trustwave Crimson	Ocean Blue	Jade Blue	Cool Grey	Powder Blue	Citrus Yellow
									
248 248 248	0 0 0	237 26 61	29 52 68	177 12 42	0 111 145	0 150 179	192 194 196	171 216 220	235 224 19
Trustwave Brand Colors Use Last				Accent Colors Use Last					

Shape and Styles



.7 5	1	2	Arrow

How to duplicate object styles

-  Select object
Ctrl + Alt + C (Copy style)
-  Select object
Ctrl + Alt + V (Paste style)
-  Outcome

Icon Examples



Check Sales Hub and the [marketing wiki page](#) for the full icon library.

Icon Examples



Check Sales Hub and the [marketing wiki page](#) for the full icon library.



Trustwave Services

Lorem ipsum dolor sit amet, consectetur adipiscing elit

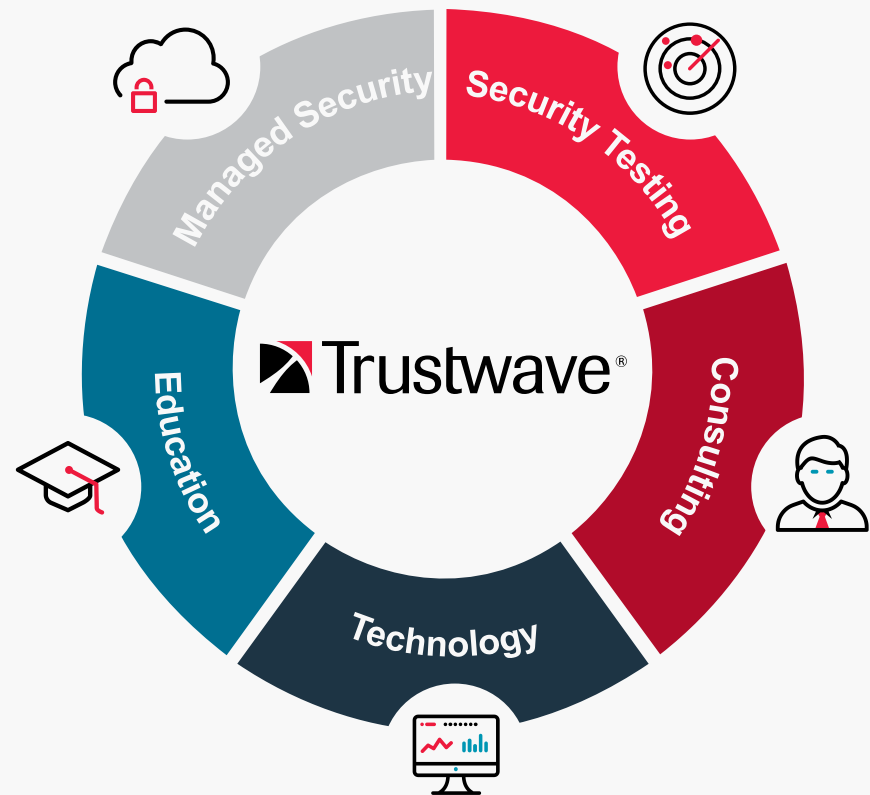
Ut gravida nulla at tortor efficitur, sit amet mattis arcu convallis

- Etiam ornare est molestie, interdum ipsum volutpat, feugiat lacus

Lorem ipsum dolor sit amet, consectetur adipiscing elit

Ut gravida nulla at tortor efficitur, sit amet mattis arcu convallis

- Etiam ornare est molestie, interdum ipsum volutpat, feugiat lacus



Trustwave Services



**Managed
Security**



**Security
Testing**



Consulting



Technology



Education

Charts and Tables

Chart Templates



Chart templates

are a convenient way to easily create consistent new charts and also align the aesthetics of legacy charts

Provided examples are:

- Column: standard
- Column: single color option
- Stacked column
- Doughnut
- Line

Examples can also be copy and pasted into other placeholders

Saving

Right click the edge of the chart object

Select “Save Chart Template”
(OSX: “Save Template”)

Appropriately name
(e.g. Column_chart)

Click “Save”

(This will have to be done once for each chart type)

Using

New in placeholder: Click the chart icon

Update legacy: Right click on the edge of the chart object, then select “Change Chart Type”

PC

Select “Template”
(on the left hand side of the popup)

Select chart

Click “Ok”

Mac (Older versions)

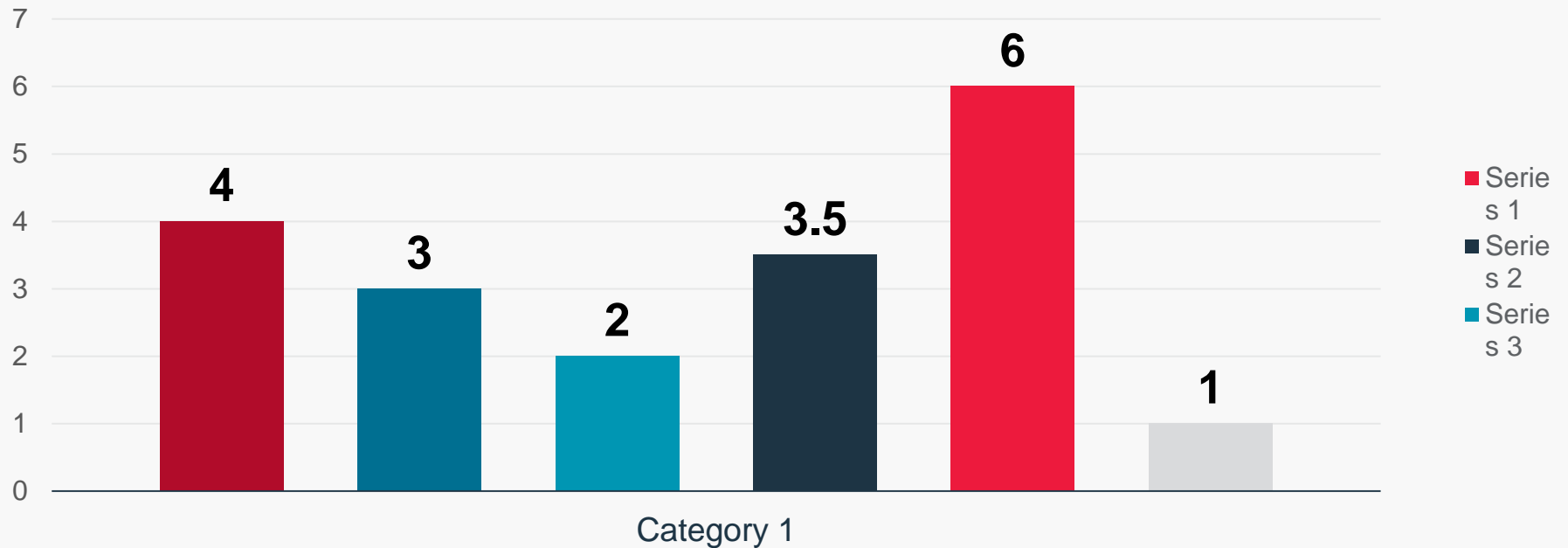
Click “Other ▼” in the Ribbon
(Scroll down to “Templates”)

Select chart

Column Chart Example



CHART TITLE PLACEHOLDER

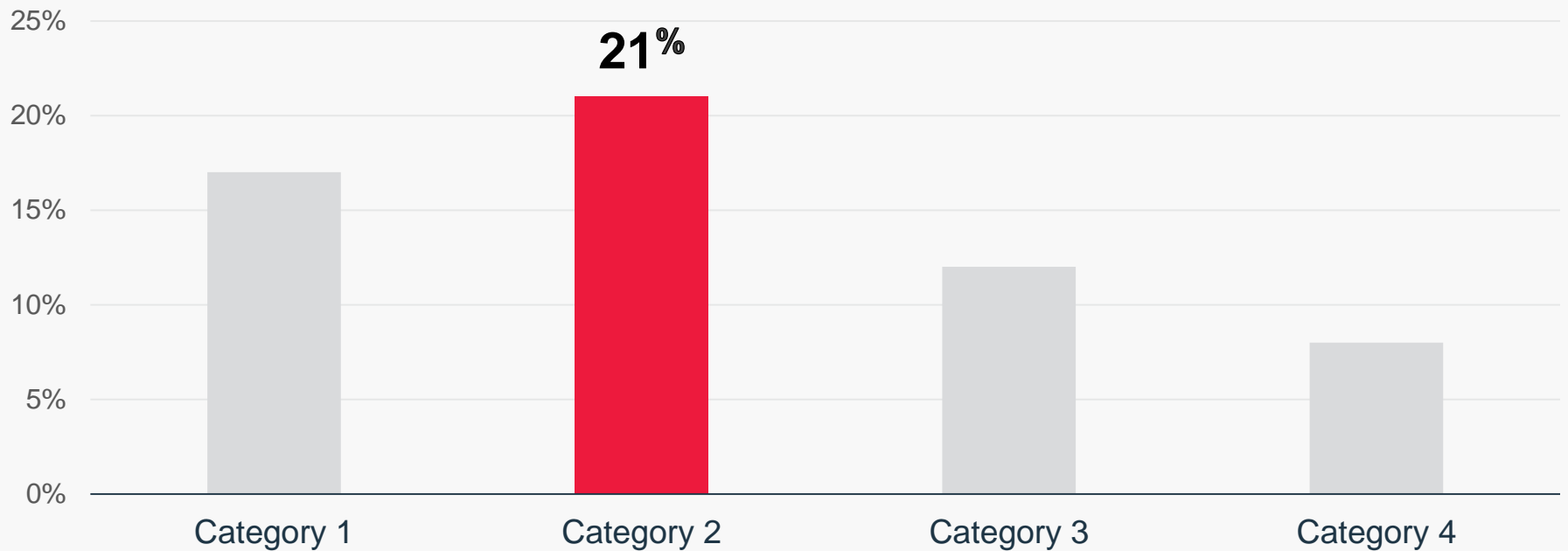


Source: placeholder

Column Chart Example

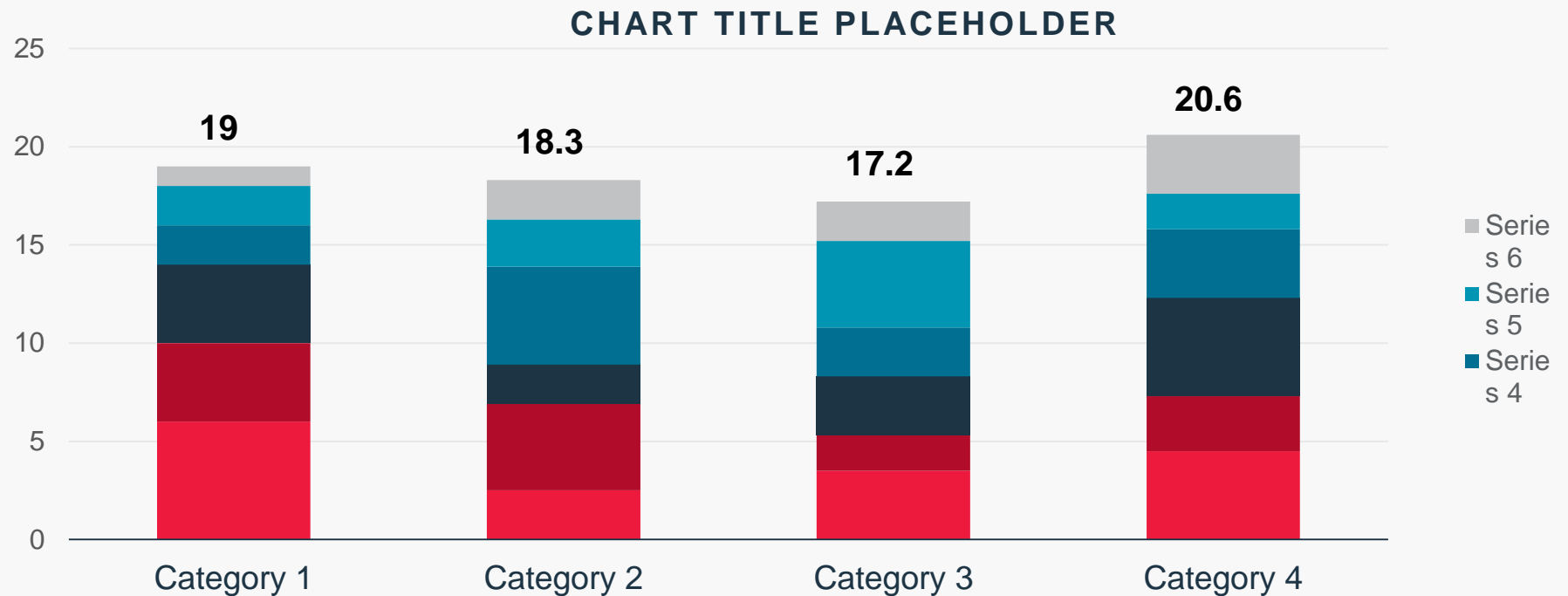


CHART TITLE PLACEHOLDER



Source: placeholder

Stacked Column Chart Example

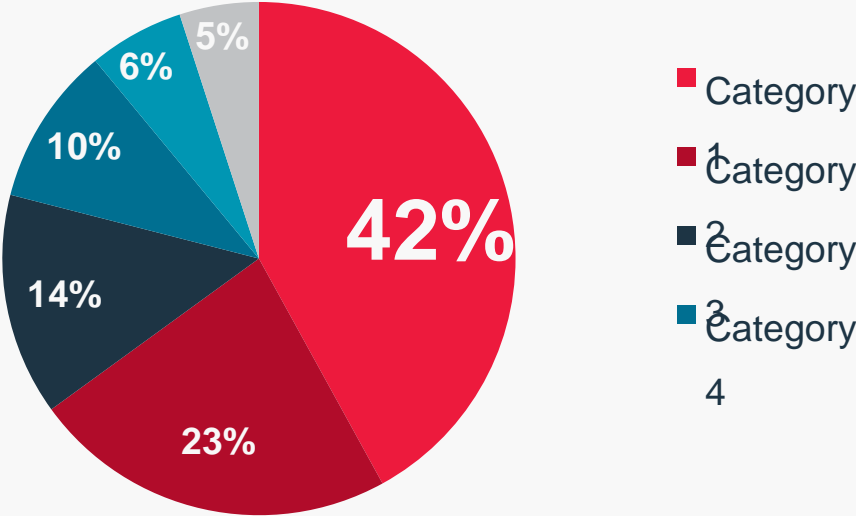


Source: placeholder

Pie Chart Example



CHART TITLE PLACEHOLDER

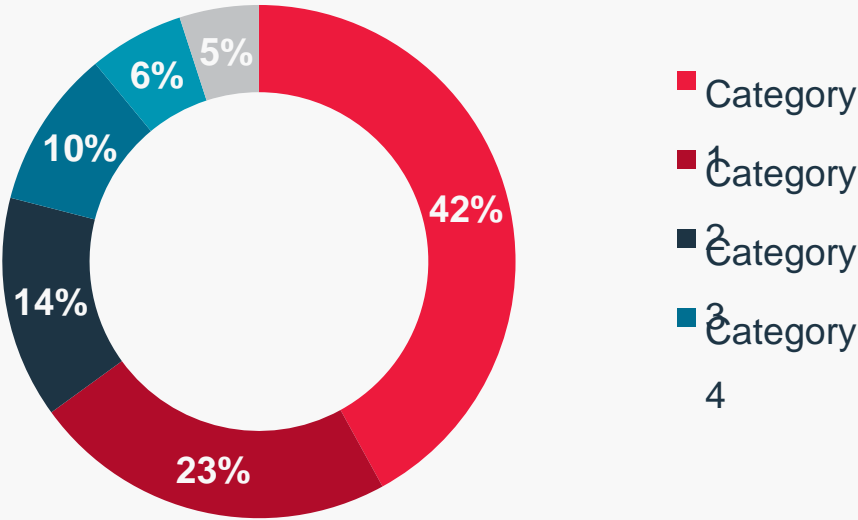


Source: placeholder

Donut Chart Example

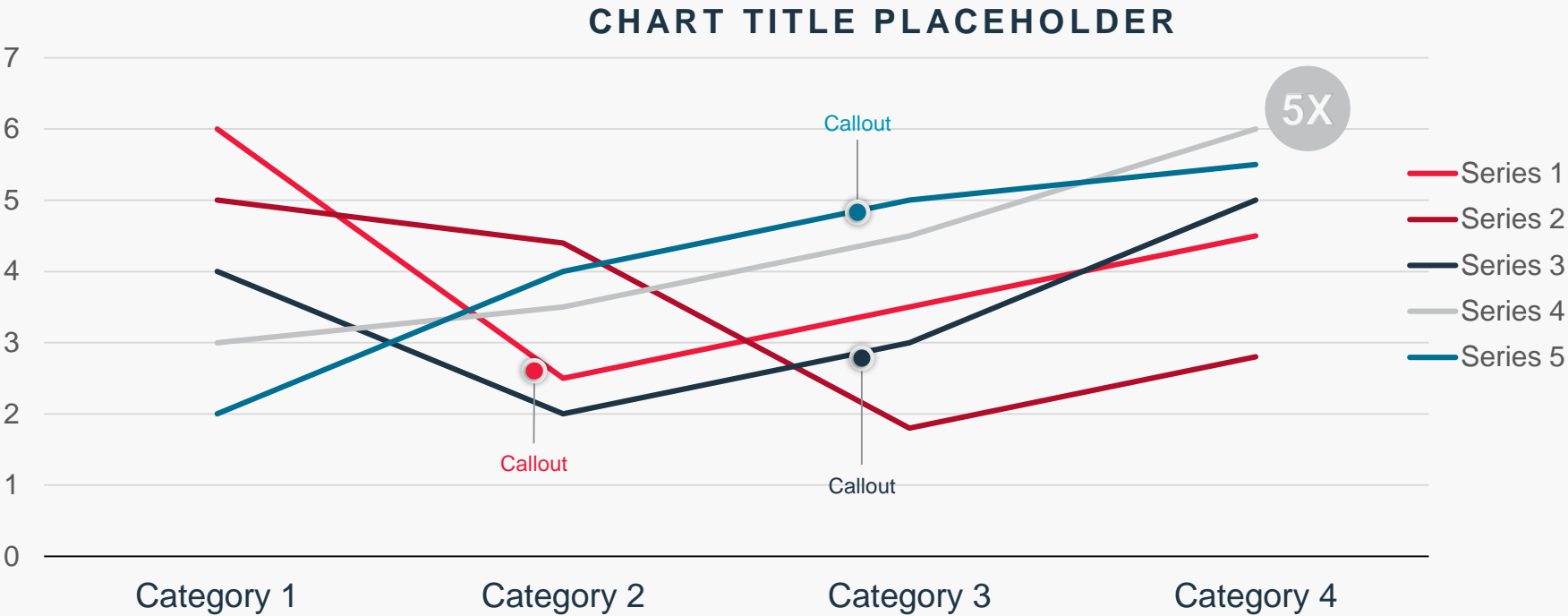


CHART TITLE PLACEHOLDER



Source: placeholder

Line Chart Example



Source: placeholder

Text Table Example



When searching for information in a table

Users expect the information to be displayed in a consistent manner. You can ensure there is consistency in the typeface of similar elements, in the alignment of similar data and in the emphasis of elements.

Highlight the most important values

Consider highlighting specific values to emphasize your message by drawing a box around the data or highlighting in a contrasting color.

Column Header

General Text Style

Bulleleted Content

Row Header

General text placeholder

- Aenean non lacinia nulla
- Nulla id semper lacus

Highlight Example

Text highlight example

- Aenean non lacinia nulla
- Nulla id semper lacus

Title Case Text

Sentence case text

- Sentence case text

16pt

14pt

- 12pt
- Ctrl + Shift + C = Copy style
- Ctrl + Shift + V = Paste style

Text Table Example



Make it easy to compare numbers

Side by side comparisons seem to be easier for people to make than above-below comparisons. In light of this, construct your tables so users will compare data between columns. In addition, the eye can run down a column rather quickly, but many people use their finger as a guide to read across rows.

Group similar data

If you can organize the data into subgroups and subcategories without altering the purpose of the table, this can improve search and make it easy to compare similar data.

Column Header	Percent Style	Monetary Style
Row Header	45%	\$200M
Highlight Example	35%	€345B
Title Case Text	68%	£34M
16pt	18pt	18pt

Slide Samples and Additional Surface Layouts



The World You Live In

Historically, law professionals have been late adopters into the security world. Recently attitudes have changed with high profile breaches, highlighting vulnerabilities that could affect any firm.

- 1 Staff Augmentation
- 2 Threat Intelligence Gap
- 3 Leverage Existing Technologies
- 4 Lack of Expertise
- 5 Untested Response Planning



By 2020, 40% of all security technology acquisitions will be directly influenced by MSSPs...up from less than 15% in 2016.

Gartner / 2017

Track Record of Success



3M+

Business subscribers

10K+

MSS customers

4M+

Vulnerability scans per year

Hundreds

**Data breach investigations
per year**

Thousands

Penetration tests per year

Billions

Events each day

Everyone Wants to Work With the Best



A Leader

Magic Quadrant: Managed security services providers.

A Leader

MarketScape: Incident response and readiness.

Winner

Best managed security services provider.

2018

Gartner[®]

2018

 **IDC** | ANALYZE THE FUTURE

2017

SC
M E D I A

Gartner, "Magic Quadrant for Managed Security Services, Worldwide" by Toby Bussa, Kelly M. Kavanagh, Pete Shoard, Sid Deshpande, February 27, 2018
IDC MarketScape U.S. Incident Readiness, Response, and Resiliency Services 2018 Vendor Assessment – Beyond the Big 5 Consultancies (Document #US44257117)



Trustwave delivers complete security to address the growing challenges you face.



Managed Security

Unmatched expertise, intelligence and customization to lend a helping hand around threat protection, detection and response



Security Testing

Skilled vulnerability hunters dig deep into IT infrastructure to weed out weaknesses before they are exploited



Consulting

Elevate maturity and mitigate risk with consulting services, from data forensics and incident response to custom testing and red teaming



Technology

Security technologies from Trustwave and other industry leaders designed to help prevent and manage threats



Education

Instill awareness, knowledge and experience on a range of topics into all members of staff, from the ground troops to the IT team to the corner offices



Trustwave delivers complete security to address the growing challenges you face.



Managed Security



Security Testing



Consulting



Technology



Education

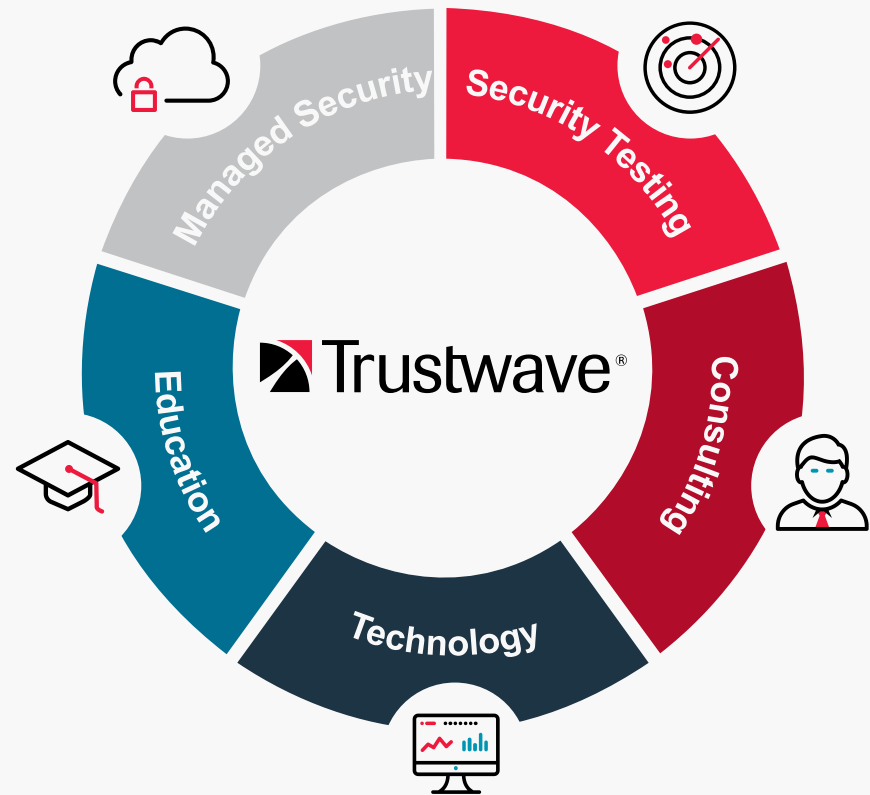


Trustwave delivers complete security to address the growing challenges you face.





Trustwave delivers complete security to address the growing challenges you face.



Operation: Grand Mars

2016-2017

Threat:

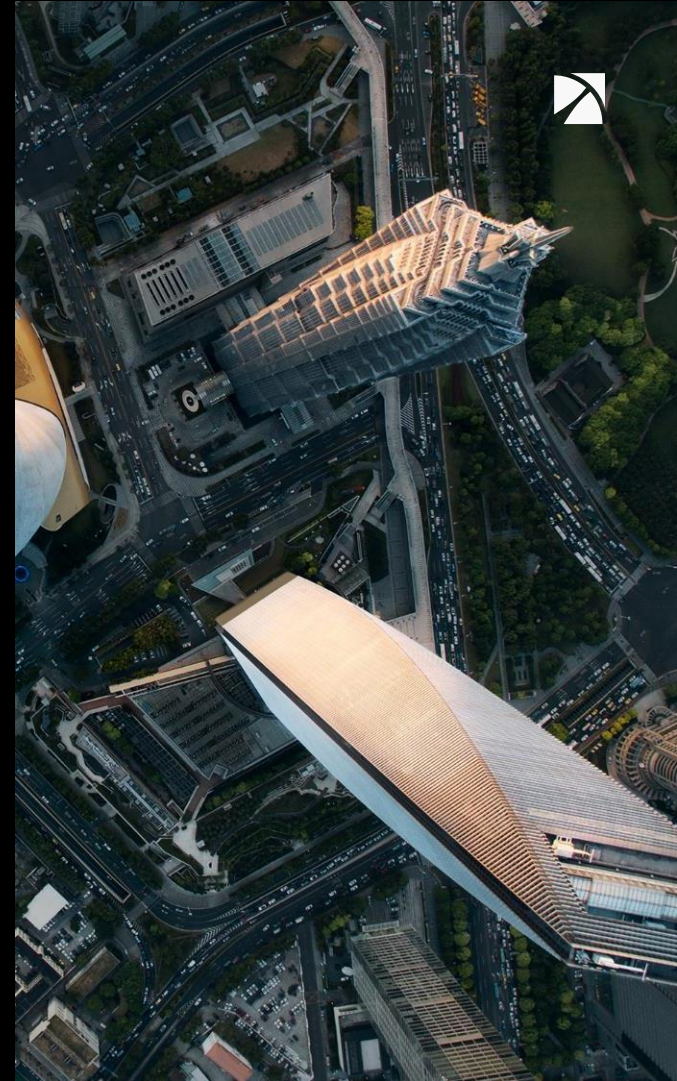
Carbanak Cybercrime Group—Responsible for theft of billions of dollars across hospitality and retail customers in Europe and North America.

Discovery:

Trustwave threat hunting service discovered Carbanak variant through proactive monitoring of hospitality customer. Targeted emails carried malicious payloads that infected, spread and breached payment systems.

Recommendation:

Trustwave worked with customers to limit damage and data loss upon discovery as part of incident response plan. Trustwave then identified other customers that were breached and collaborated with FBI to investigate and prosecute cybercrime group.



DHG

DIXON HUGHES GOODMAN LLP

Cloud Readiness & Governance



Agenda

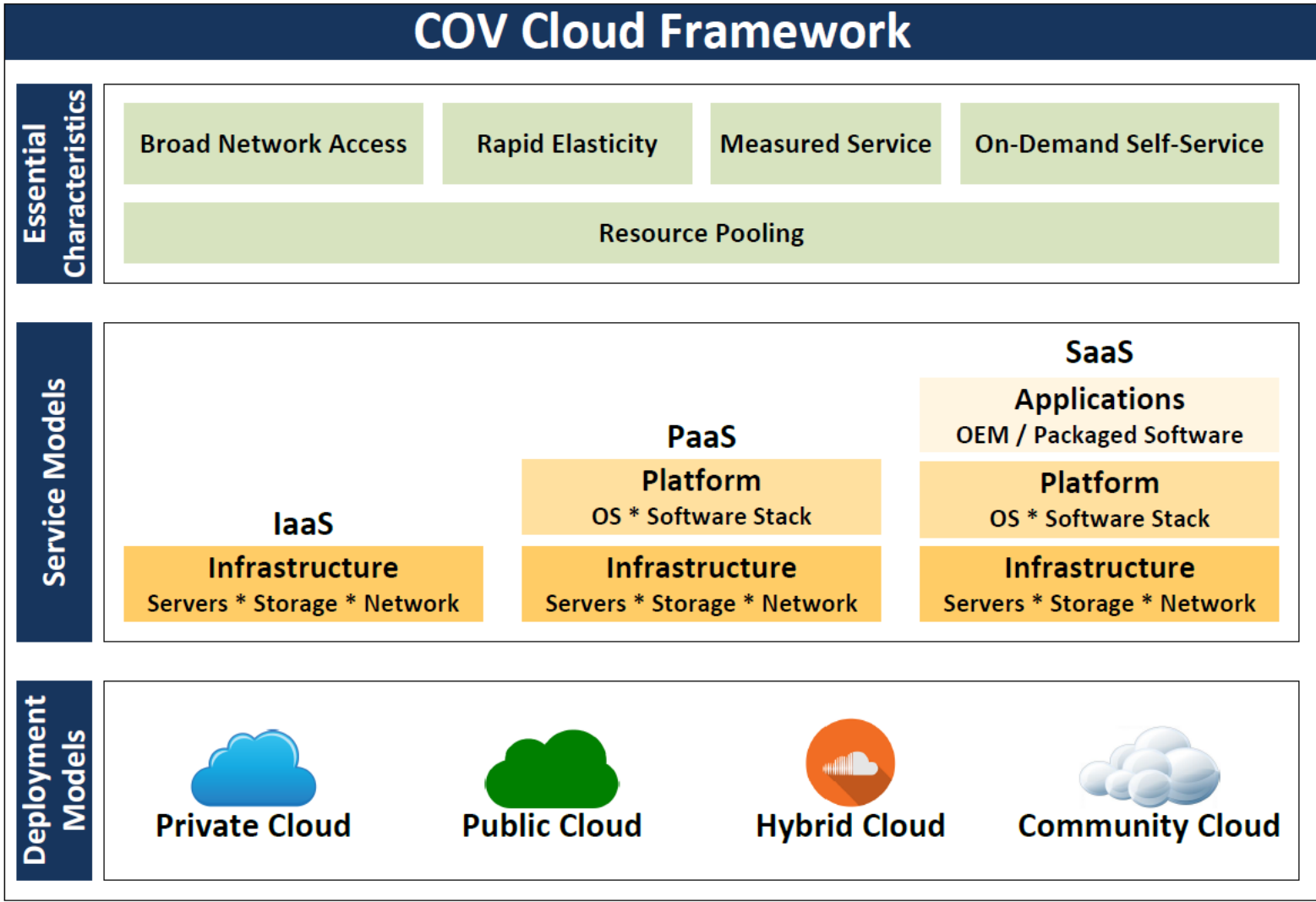
1. COV Cloud Service Models, Deployment Models, & Expected Outcomes
2. Cloud Readiness Tips and Governance

DHG

DIXON HUGHES GOODMAN LLP

Cloud Service Models, Deployment Models, & Expected Outcomes

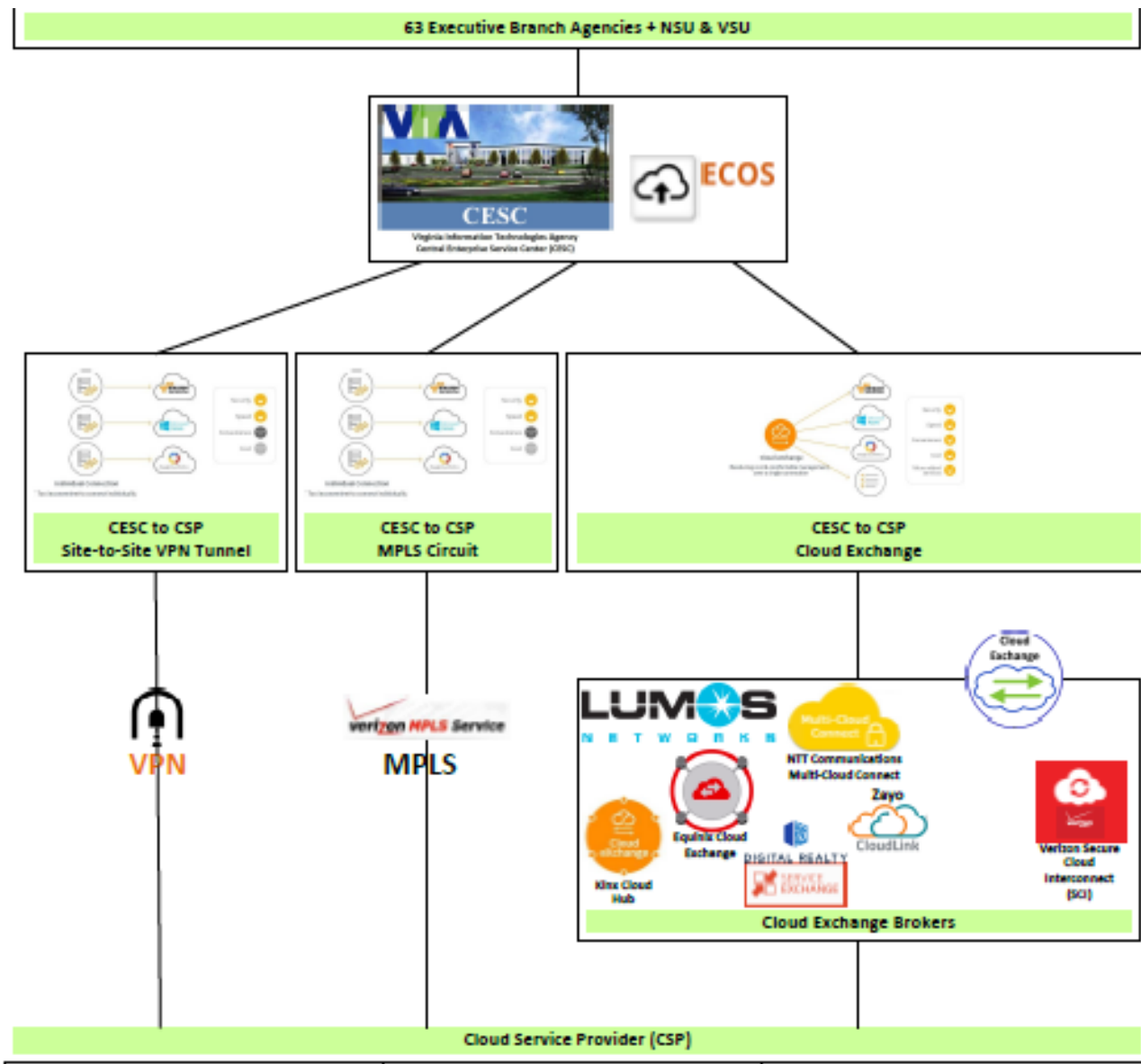
COV Cloud Framework



Ver-2.3: October 23, 2018



COV Cloud Connection Options



DHG

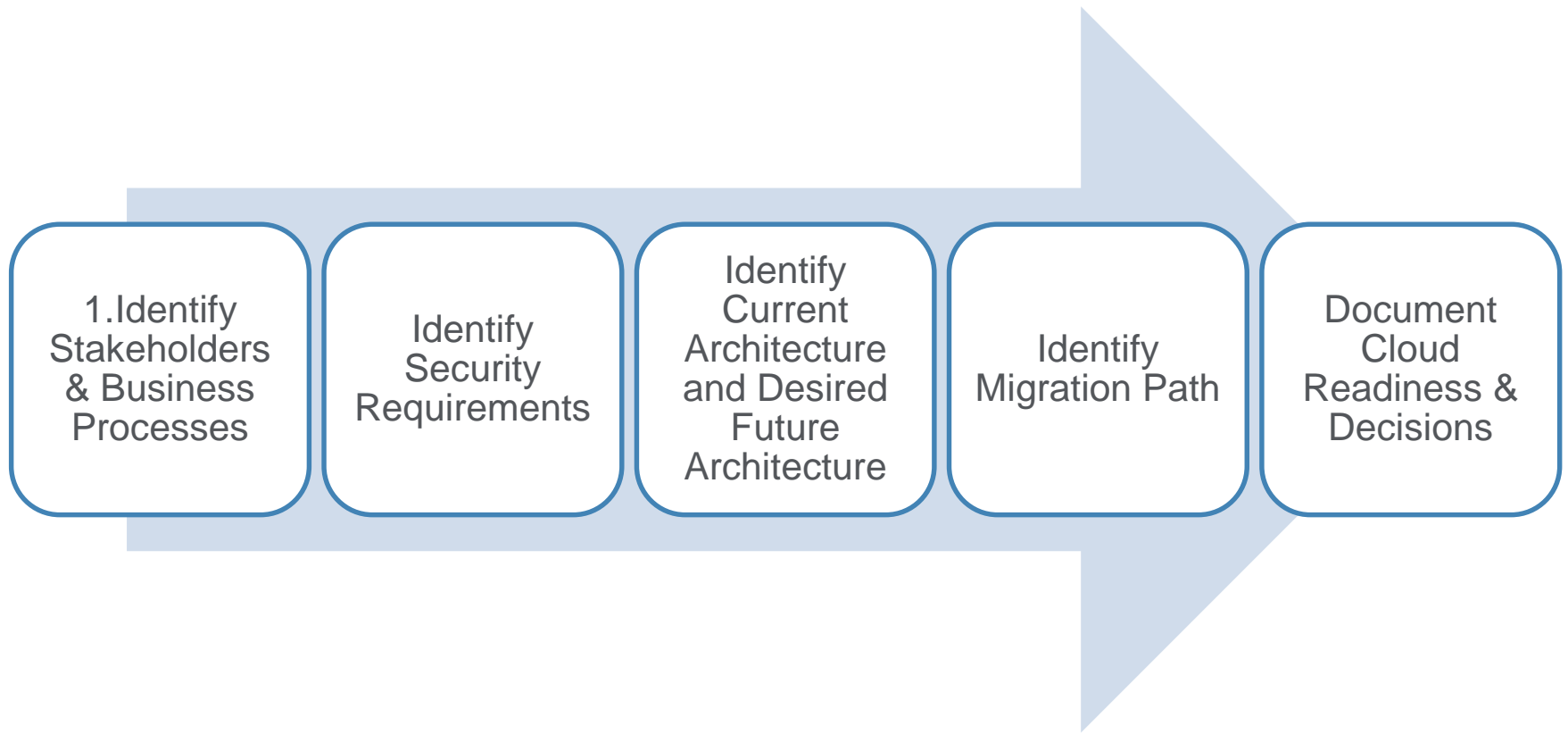
DIXON HUGHES GOODMAN LLP

Cloud Readiness Tips and Governance

Cloud Governance



Cloud Readiness





Virginia Information Technologies Agency

**Last 4 slides of this
presentation have
been deleted due to
security reasons**





Virginia Information Technologies Agency

Upcoming Events





2020 COV Security Conference

2020 Security Conference Registration and Call for Papers

Registration for the 2020 Commonwealth of Virginia (COV) Information Security Conference will open later this month. The 2020 conference will be held April 16 & 17 at the Altria Theater in Richmond. The call for papers has been issued and the conference committee is now accepting submissions thru the VITA website.

Conference and registration information can be found on the link below.

<https://www.vita.virginia.gov/commonwealth-security/cov-is-council/cov-information-security-conference/>

Send your call for papers questions to: isconferencecfp@vita.virginia.gov

For all other conference questions: covsecurityconference@vita.virginia.gov



Future ISOAG

February 5 , 2020 @ CESC 1:00-4:00

Speakers: Samuel "Gene" Fishel – OAG

Brett Kourey – RiskLens

Beth Waller – Woods Rogers PLC

ISOAG meets the 1st Wednesday of each month in 2019

ADJOURN

THANK YOU FOR ATTENDING

