

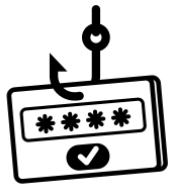


# Reducing the Fog of Cyber Warfare

## Incident Response

Cyber Security Summit NAB 2019

Janice Pearson VP, Global Content Protection &  
Mathew Gilliat-Smith, Advisor, Convergent Risks



# Typical Incidents

**Email Phishing** attack

**Attrition** attack on IP address/server

**Freelancer blog** plot revealed

**Pre-Theatrical Release** prior to embargo

**Web - Malware Infections**

**Loss or Theft** of equipment e.g. laptop or smartphone trailer Leaks

**Improper Usage** - violation of acceptable usage policies. Post 'off-boarding'

**Other** - Client photography in theatre, break-In

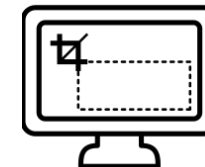
# Limitations of Manual Incident Response

- A lot of info - reliance on **emails**, **Excel**, **Word**, screen shots - complex to assemble – different **versioning**
- **Blocked emails** through filtering
- Generally **reliant on one or two individuals** for the information
- IT ticketing systems – issues with internal **confidentiality**
- **Scramble to assimilate**, analyze, communicate & act
- Key parts **overlooked**



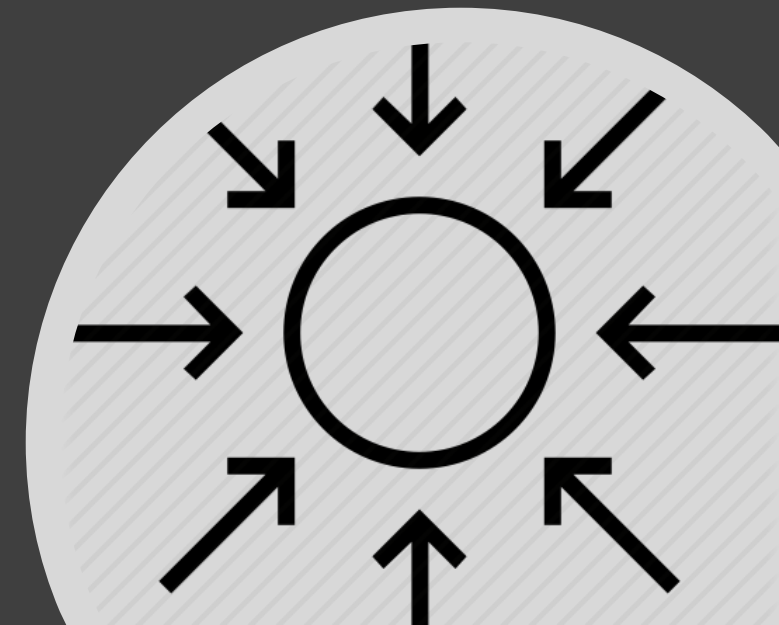
**COMPANY**  
**Security Incident Timeline - Internal**  
STRICTLY PRIVATE AND CONFIDENTIAL

Date	Time	Actions	Notes	Sender	Receiver	Communication method	Evidence reference
11/01/18	16:30:00	ME emails NAME [JG] with basic notification details and information. 16:33	NAME [ME] receives phone call from Appco employee, notifying her that an amount of COMPANY's supporter personal data has been distributed by accident by a [JG].	NAME [KMcK] Appco Employee	NAME	Phone Call	n/a
11/01/18	16:33:00	DPO notification	Data Protection Officer at COMPANY.	[ME]	[JG]	Email	email id
11/01/18	16:40:00	Phone call to discuss incident	verbally	[JG]	[ME]	Phone Call	n/a
11/01/18	17:36:00	[JG] responds with an email	<ul style="list-style-type: none"> <li>• Not sure what the 18 refers to. How many Australian supporters was this sent to? Also how many COMPANY supporters</li> <li>• You quite rightly ask how they know - this should cover how they were made aware</li> <li>• Confirmation of how happened</li> <li>• Could there be a risk that any more Appco supporters or COMPANY's supporters affected?</li> <li>• What are they doing to prevent this recurring?</li> <li>• Description of details disclosed</li> <li>• Confirmation they have removed all details from their Executive incident summary from Appco</li> </ul>	[JG]	[ME] [PM] [SU]	Email	email id
11/01/18	18:04:00	[ME] receives email	Requests more information	[KMcK]	[ME]	Email	email id
12/01/18	09:31:00	[ME] responds	Internal discussion on incident response. Conclude that ICO should be notified and 18x affected donors should be notified. [BB] to confirm ICO notification advice with Protection and Claire Horton [CH] should be made aware ICO notification. Fundraising team to start to notify affected donors of	[ME]	[KMcK]	Email	email id
12/01/18	11:10:00	[JG], [ME], [PM] & Ben Bradley [BB] meet	Phone call, followed up with email	Fundraising support team	18x affected donors	Face to Face	n/a
12/01/18	11:15:00	Fundraising Team start to contact 18x affected donors	Speaks with Gary Simpson [GS] who confirms best practise to [ME], [BB], [KMcK] and NAME. Operations Director (Appco). Executive summary of incident.	[BB]	[GS]	Phone Call	n/a
12/01/18	13:00:00	[BB] calls Protection					



# Central Incident Response Management Platform

- **Centralized ticketing** system segregated from the network
- Incident Response - a discipline of **Continual Improvement** better Analysis to convert volumes of data into actionable intelligence and evidence
- **Faster Response** and recovery managing security incidents in real time
- **Contained Communication** - hierarchy of user permission levels - need to know basis. Emails containing IP address not blocked as suspicious
- **Encrypted Data**, immutably stored for analyst investigation & legal
- **No PII issues** – Personal Data is not distributed outside of the platform: CCPA GDPR
- **Malware evidence** stored hashed and encrypted



# Home Dash Board

- Information & Status
- Incident Snap Shot
  - with real time data with tasks, activity
- View Assets
- Add users, permissions
- Communication

## My Home



## My Tasks

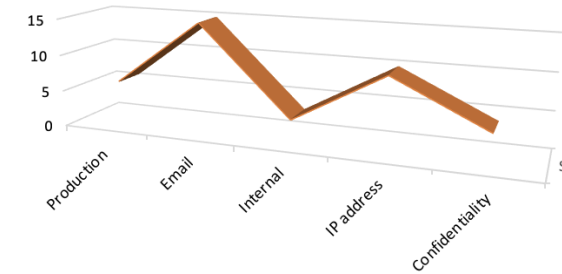


## While you were away

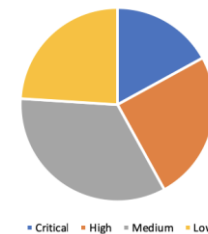
Notifications panel showing a list of messages with timestamps and actions.

Time	Message
7 minutes ago	Tina Operations has begun work on your task: 'Ensure attendee has acknowledged appropriate NDA' in incident: 'Unauthorized screen shot'
7 minutes ago	You have been assigned task 'Follow up with Account Management' in incident 'Unauthorized screen shot' by 'Tina Operations'
7 minutes ago	You have been assigned task 'Ensure attendee has acknowledged appropriate NDA' in incident 'Unauthorized screen shot' by 'Tina Operations'
8 minutes ago	Tina Operations has begun work on your task: 'Watermark screen grab' in incident: 'Unauthorized screen shot'
13 minutes ago	You have been assigned task 'Watermark screen grab' in incident 'Unauthorized screen shot' by 'Tina Operations'

## Incidents in last 7 days



## Threat Levels

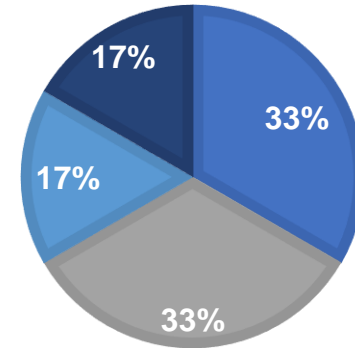


# Analysis of Activity

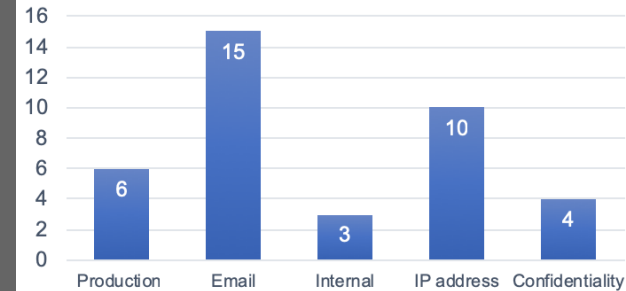
- Analysis
  - Graphs, charts, timelines
- A Playbook Feature
  - Visual representation for activity and remediation steps
  - Playbook Designer – drag & drop, add steps
  - Save to library & publish
  - Add playbook into an existing incident with Playbook Wizard

## STATUS OF INCIDENTS

■ Critical ■ High ■ Medium ■ Low



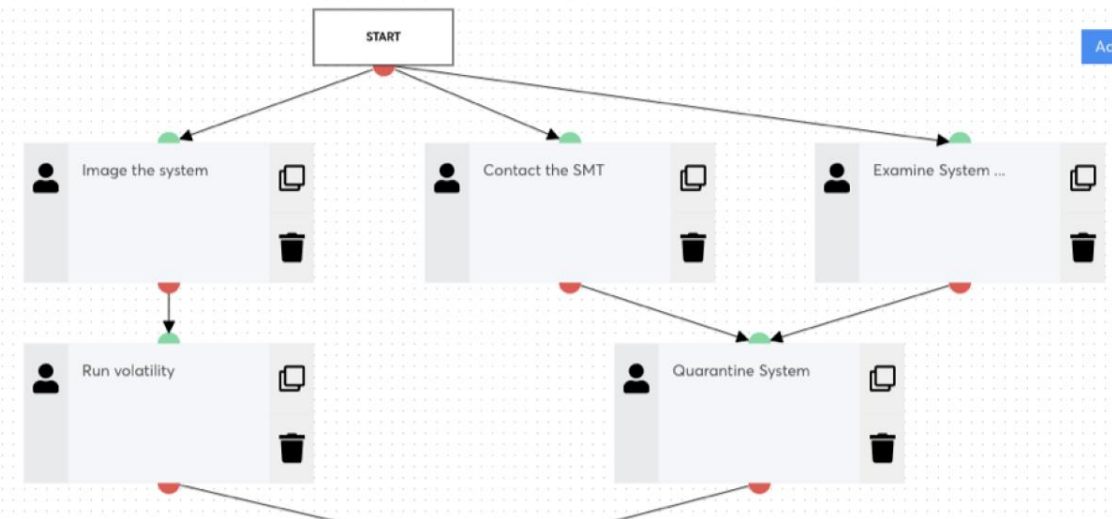
## Incidents By Type



## Malware

Created by on 18th of January 1970

Edit Title Delete Save Publish



VERSION PREVIEW

# Clients, Users, Permissions

- **User permissions**
  - who is allowed to see what when
- **Teams** – set & edit permission levels
  - Enterprise Analysts: **central control**
  - Analysts: e.g. create **tasks but not incidents**, upload, examine, search evidence
  - Contributors (in the field) e.g. access to a single group, can **upload evidence only**

Action	System Admin	Enterprise Analyst	Analyst	Incident Contributor
<i>System</i>				
View Authentication Logs	✓			
View Activity Logs	✓			
Assign SSL Certs	✓			
Private Message Users	✓	✓	✓	✓
<i>Clients</i>				
Create Clients	✓	✓		
Edit Clients	✓	✓		

Add Type

Type name\* Type

Area\* --- Choose area ---

- Asset/Entity Additional Information
- Asset Group
- Compromised Accounts Type
- Asset/Entity Status
- Asset/Entity Device Type
- Incident Type
- Asset/Entity Operating System
- Asset/Entity Operating System Version
- Incident Status

# Adding Incidents & Evidence

- **Import Incidents**

- Wizard to add, create, edit ensures all steps are completed
- Event logs
- Assets: laptops, servers, desktops, server rooms, buildings, IP addresses, malware sites

- **Evidence**

- Uploading, downloading, analyzing
- Encrypted in transit at rest
- Ghost evidence (with hashing to original path & ASCII Strings)
- Virus Total for file integrity

1 Details 2 Notes 3 Users 4 Playbooks 5 Tasks 6 Briefing 7 Finish

**Briefing**

If you want to send an initial email out enable the send briefing option and fill in the recipients, subject and message fields.

Send briefing:

Recipients  
Select option

Subject

Message  
Sans Serif Normal B I U S A H1 H2 H3 H4 H5 H6 H7 H8 H9 H10 H11 H12 H13 H14 H15 H16 H17 H18 H19 H20 H21 H22 H23 H24 H25 H26 H27 H28 H29 H30 H31 H32 H33 H34 H35 H36 H37 H38 H39 H40 H41 H42 H43 H44 H45 H46 H47 H48 H49 H50 H51 H52 H53 H54 H55 H56 H57 H58 H59 H60 H61 H62 H63 H64 H65 H66 H67 H68 H69 H70 H71 H72 H73 H74 H75 H76 H77 H78 H79 H80 H81 H82 H83 H84 H85 H86 H87 H88 H89 H90 H91 H92 H93 H94 H95 H96 H97 H98 H99 H100 H101 H102 H103 H104 H105 H106 H107 H108 H109 H110 H111 H112 H113 H114 H115 H116 H117 H118 H119 H120 H121 H122 H123 H124 H125 H126 H127 H128 H129 H130 H131 H132 H133 H134 H135 H136 H137 H138 H139 H140 H141 H142 H143 H144 H145 H146 H147 H148 H149 H150 H151 H152 H153 H154 H155 H156 H157 H158 H159 H160 H161 H162 H163 H164 H165 H166 H167 H168 H169 H170 H171 H172 H173 H174 H175 H176 H177 H178 H179 H180 H181 H182 H183 H184 H185 H186 H187 H188 H189 H190 H191 H192 H193 H194 H195 H196 H197 H198 H199 H200 H201 H202 H203 H204 H205 H206 H207 H208 H209 H210 H211 H212 H213 H214 H215 H216 H217 H218 H219 H220 H221 H222 H223 H224 H225 H226 H227 H228 H229 H230 H231 H232 H233 H234 H235 H236 H237 H238 H239 H240 H241 H242 H243 H244 H245 H246 H247 H248 H249 H250 H251 H252 H253 H254 H255 H256 H257 H258 H259 H260 H261 H262 H263 H264 H265 H266 H267 H268 H269 H270 H271 H272 H273 H274 H275 H276 H277 H278 H279 H280 H281 H282 H283 H284 H285 H286 H287 H288 H289 H290 H291 H292 H293 H294 H295 H296 H297 H298 H299 H300 H301 H302 H303 H304 H305 H306 H307 H308 H309 H310 H311 H312 H313 H314 H315 H316 H317 H318 H319 H320 H321 H322 H323 H324 H325 H326 H327 H328 H329 H330 H331 H332 H333 H334 H335 H336 H337 H338 H339 H340 H341 H342 H343 H344 H345 H346 H347 H348 H349 H350 H351 H352 H353 H354 H355 H356 H357 H358 H359 H360 H361 H362 H363 H364 H365 H366 H367 H368 H369 H370 H371 H372 H373 H374 H375 H376 H377 H378 H379 H380 H381 H382 H383 H384 H385 H386 H387 H388 H389 H390 H391 H392 H393 H394 H395 H396 H397 H398 H399 H400 H401 H402 H403 H404 H405 H406 H407 H408 H409 H410 H411 H412 H413 H414 H415 H416 H417 H418 H419 H420 H421 H422 H423 H424 H425 H426 H427 H428 H429 H430 H431 H432 H433 H434 H435 H436 H437 H438 H439 H440 H441 H442 H443 H444 H445 H446 H447 H448 H449 H450 H451 H452 H453 H454 H455 H456 H457 H458 H459 H460 H461 H462 H463 H464 H465 H466 H467 H468 H469 H470 H471 H472 H473 H474 H475 H476 H477 H478 H479 H480 H481 H482 H483 H484 H485 H486 H487 H488 H489 H490 H491 H492 H493 H494 H495 H496 H497 H498 H499 H500 H501 H502 H503 H504 H505 H506 H507 H508 H509 H510 H511 H512 H513 H514 H515 H516 H517 H518 H519 H520 H521 H522 H523 H524 H525 H526 H527 H528 H529 H530 H531 H532 H533 H534 H535 H536 H537 H538 H539 H540 H541 H542 H543 H544 H545 H546 H547 H548 H549 H550 H551 H552 H553 H554 H555 H556 H557 H558 H559 H560 H561 H562 H563 H564 H565 H566 H567 H568 H569 H570 H571 H572 H573 H574 H575 H576 H577 H578 H579 H580 H581 H582 H583 H584 H585 H586 H587 H588 H589 H590 H591 H592 H593 H594 H595 H596 H597 H598 H599 H600 H601 H602 H603 H604 H605 H606 H607 H608 H609 H610 H611 H612 H613 H614 H615 H616 H617 H618 H619 H620 H621 H622 H623 H624 H625 H626 H627 H628 H629 H630 H631 H632 H633 H634 H635 H636 H637 H638 H639 H640 H641 H642 H643 H644 H645 H646 H647 H648 H649 H650 H651 H652 H653 H654 H655 H656 H657 H658 H659 H660 H661 H662 H663 H664 H665 H666 H667 H668 H669 H670 H671 H672 H673 H674 H675 H676 H677 H678 H679 H680 H681 H682 H683 H684 H685 H686 H687 H688 H689 H690 H691 H692 H693 H694 H695 H696 H697 H698 H699 H700 H701 H702 H703 H704 H705 H706 H707 H708 H709 H710 H711 H712 H713 H714 H715 H716 H717 H718 H719 H720 H721 H722 H723 H724 H725 H726 H727 H728 H729 H730 H731 H732 H733 H734 H735 H736 H737 H738 H739 H740 H741 H742 H743 H744 H745 H746 H747 H748 H749 H750 H751 H752 H753 H754 H755 H756 H757 H758 H759 H760 H761 H762 H763 H764 H765 H766 H767 H768 H769 H770 H771 H772 H773 H774 H775 H776 H777 H778 H779 H780 H781 H782 H783 H784 H785 H786 H787 H788 H789 H790 H791 H792 H793 H794 H795 H796 H797 H798 H799 H800 H801 H802 H803 H804 H805 H806 H807 H808 H809 H810 H811 H812 H813 H814 H815 H816 H817 H818 H819 H820 H821 H822 H823 H824 H825 H826 H827 H828 H829 H830 H831 H832 H833 H834 H835 H836 H837 H838 H839 H840 H841 H842 H843 H844 H845 H846 H847 H848 H849 H850 H851 H852 H853 H854 H855 H856 H857 H858 H859 H860 H861 H862 H863 H864 H865 H866 H867 H868 H869 H870 H871 H872 H873 H874 H875 H876 H877 H878 H879 H880 H881 H882 H883 H884 H885 H886 H887 H888 H889 H890 H891 H892 H893 H894 H895 H896 H897 H898 H899 H900 H901 H902 H903 H904 H905 H906 H907 H908 H909 H910 H911 H912 H913 H914 H915 H916 H917 H918 H919 H920 H921 H922 H923 H924 H925 H926 H927 H928 H929 H930 H931 H932 H933 H934 H935 H936 H937 H938 H939 H940 H941 H942 H943 H944 H945 H946 H947 H948 H949 H950 H951 H952 H953 H954 H955 H956 H957 H958 H959 H960 H961 H962 H963 H964 H965 H966 H967 H968 H969 H970 H971 H972 H973 H974 H975 H976 H977 H978 H979 H980 H981 H982 H983 H984 H985 H986 H987 H988 H989 H990 H991 H992 H993 H994 H995 H996 H997 H998 H999 1000

Insert text here ...

malicious.js

Awaiting Analysis

Details View File Strings Check Virus Total (requires internet connecti) Download

Author: Tasha Godwin (tasha@logicallysecure.com)

File Location: Cyber CPR Secure Vault

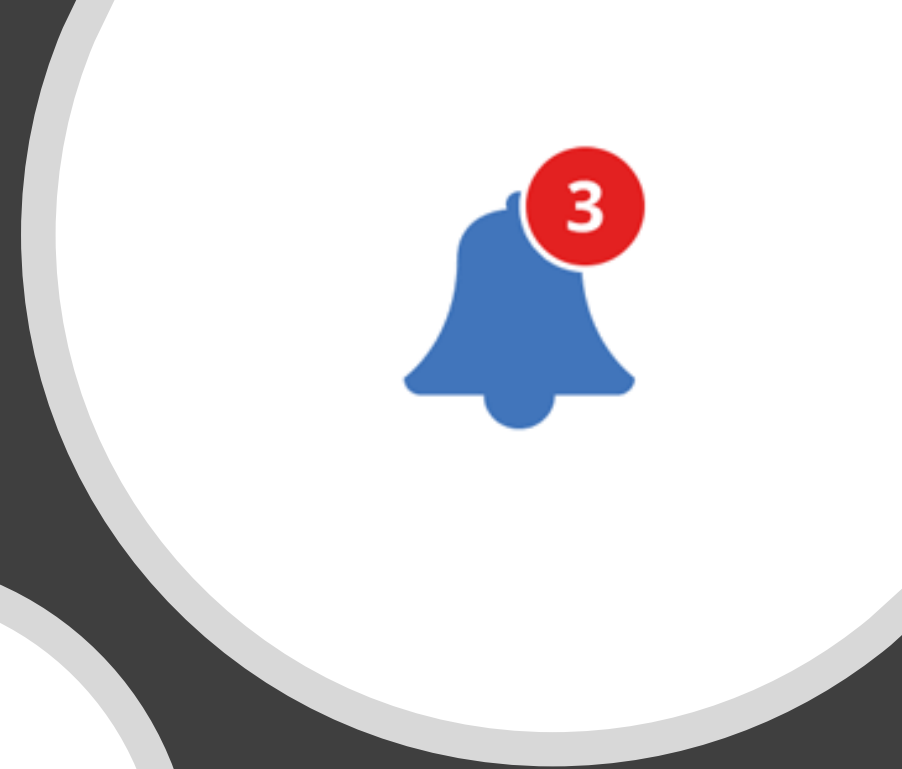
Associated Entity: Desktop

Awaiting Analysis  
Undergoing Analysis  
Unable to Verify  
Verified as Malicious  
Verified as Not Malicious



# Searches & Alerts

- **Search tool** for all incidents and clients
- By ASCII strings
- **Alerts Icon** – notify managers & users to priority events
- **Save so much time** with all assets logged in one repository



# Incident Processing

- Running Analysis
  - GREP to search strings
  - Volatility to analyze Windows memory images
- Observables
  - Non physical i.e. IP addresses, hashes to trace attacker activity & identify victim machines
- Indicators - Host & Network based to act on intelligence
- Compromised Accounts - record & monitor
- Convert Documents to Evidence

The screenshot shows the 'Evidence' interface with a navigation bar at the top containing: Dashboard, Entities, Evidence (selected), Observables, Compromised Accounts, Notes, Tasks, Documents, Comms, Messaging, Playbooks, Users, Chat, and Settings. Below the navigation bar, there are three evidence items represented as blue boxes: 'pslist' (volatility command), '46' (processes), and 'matt' (conducted this analysis). To the right of these items is a metadata panel for the selected item, showing: TYPE: Volatility, FILE: xp-laptop-2005-06-25.img, DATE: Today at 3:58 PM, and ACTIONS: Import as evidence and Delete. Below the metadata panel is a table with the following columns: OFFSET(V), NAME, PID, PPID, THDS, HNDS, SESS, WOW64, START, and EXIT. The table contains three rows of process data.

OFFSET(V)	NAME	PID	PPID	THDS	HNDS	SESS	WOW64	START	EXIT
0xB23c87c0	System	4	0	61	1140	-----	0		
0x81fd020	smss.exe	448	4	3	21	-----	0	2005-06-25 16:47:28 UTC+0000	
0x81f5a3b8	csrss.exe	504	448	12	596	0	0	2005-06-25 16:47:30 UTC+0000	

The screenshot shows a dialog box titled 'Convert Document to Evidence' with a warning icon. Below the title, there is a message: 'Once you have converted the incident document to evidence it cannot be removed.' At the bottom right of the dialog, there are two buttons: 'Confirm' (green) and 'Cancel' (red).

# Communication, Messaging & Chat

- Chat between assigned users to same incident is immutable
- Email Templates & configuration for messaging with specific layouts e.g. adding legal disclaimers
- Wizard for customized event briefings
- Accuracy & Proofing checks
- Briefing notices
- Communication logs
- Ideal for legal evidence

The screenshot shows a chat window for an incident titled "Insider Threat". The chat is initiated by Peter Lombardelli. The message history shows three messages: a request for analysis status, a confirmation of no malware found, and a request for further investigation. The interface includes a "Channels" sidebar with options like "# Default Incident Chat", "# Analysts", and "# Senior Managers". An "About" panel on the right lists channel and user information, including an "Add member" button and a list of potential members.

Sender	Message	Timestamp
Peter Lombardelli	Please could you report on the status of the analysis being undertaken	2018-11-15 19:39:55 (UTC)
Fred Smith	Yes, it all looks OK so far - no malware or compromise found	2018-11-15 19:45:41 (UTC)
Fred Smith	OK - please get back to me if you find anything - eyes on this one	2018-11-15 19:46:32 (UTC)

The screenshot shows a "Choose Template" dialog box with a close button (X) in the top right corner. A dropdown menu is open, showing "Please select one" and "Incident Briefing Notice" (which is selected with a checkmark). At the bottom of the dialog, there are "Cancel" and "Generate Draft" buttons.

# Summary

- Company is **better equipped** to handle an incident emergency
- More information to analyze and **more intelligence** to act on
- Less reliant on **a few individuals**
- **Faster** response times
- **Cost savings** through prevented incidents



# Case Study

- Featured in the current **SANS training** course 504
- Used by corporate, **government**, military and law enforcement in the US, UK, EU, and Australasia including DOD
- Adopted by Convergent as a **partnership offering**





- Risk assessment & compliance services
- Principal provider of TPN assessments
- Penetration & vulnerability testing
- Pre-assessments & remediation advice
- Policy development, security training, breach investigations,
- CCPA & GDPR compliance testing

[info@convergentrisks.com](mailto:info@convergentrisks.com)

Q&A