Journalist Fellowship Paper

Securing newsrooms against digital threats: lessons from new media innovators

By Paul Farrell

Published: August 2022

Fellowship: Trinity Term 2022

Sponsor: ABC

Contents

Introduction

In November 2013, I was summoned into a dark office in Sydney by then editor-in-chief of *Guardian Australia*, Katharine Viner.

“Paul, Alan needs a hand with something,” she said. “Can you pop in for a quick chat? No phones.”

I was nervous. It was very early in my career: I was 23 and had just joined *Guardian Australia* as a casual reporter. I was as low down the ladder as you can get. Alan, of course, was Alan Rusbridger, who at that time was the editor of the whole of the *Guardian*. He was in Sydney to survey the British daily’s latest expansion.

What I didn’t yet know as I walked into that office and closed the door was that there was a little more to his journey. As I sat down, he pulled out a laptop, stuck an encrypted drive into it and pulled up the screen.

This was the problem: the encrypted drive wouldn’t open. I had used that particular encryption program before, and I had been asked to help.

I was, quite frankly, terrified to be sitting in a room with about as close to a journalistic deity as you can get. I troubleshot as best I could, and, eventually, the drive opened.

Alan tried again, and a few moments later, the encrypted drive opened. He clicked on a file, and a slide with the words “TOP SECRET” opened up on the page.

“What do you think?” Rusbridger said.

I panicked. I was 23 and not even remotely equipped for this. All I could think was to stammer something embarrassingly obvious: “I think this is really big.”

Unwittingly, I had become the first Australian, outside of a handful of intelligence operatives, to see the documents obtained by Edward Snowden that revealed the extent of Australia's surveillance on the head of state of its nearest neighbour, Indonesia. When the story was published by the Guardian in collaboration with the ABC some weeks later, it generated a political and diplomatic storm that raged for weeks.

Sitting in that small office with Rusbridger was a formative moment for my understanding of what kind of skills journalists in a digital age need to have. The bit part I played clarified for me the importance of becoming adept at wielding these new tools that could help us protect ourselves and our sources – something I would later come to recognise as the building blocks for a strong information security culture in a newsroom.

I threw myself into learning more about surveillance and how to counter it. I worked on how best I could incorporate the increasing number of tools at our disposal into my workflow. I learned more about the capabilities of digital surveillance, how individual devices could be enslaved in all kinds of nefarious ways, and the ways to fight it.

My colleagues at the *Guardian*'s Australian office thought I was crazy. A running joke had developed about how I thought the guy who watered the plant might actually be a spook. Another colleague was fond of suggesting that I myself may have been an intelligence agent, pointing out the curious timing with which I'd brought my skill set into the newsroom.

I was definitely paranoid, but with good reason. A few years later, I discovered the Australian federal police had accessed my phone records in an effort to identify my sources in an investigation into Australian leaks.[1]

[1] Meade, A. (2016). 'Federal Police Admit Seeking Access to Reporters Metadata Without Warrant', *The Guardian* 14 April. Available at: https://www.theguardian.com/world/2016/apr/14/federal-police-admit-seeking-access-to-reporters-metadata-without-warrant (Accessed on 27 June 2022)

Had I not been using the range of the techniques I had learnt, I am certain my sources would have been discovered. A year later, when I led a team of reporters to publish the Nauru files – the largest leak of documents from inside Australia's offshore detention regime – one of the first reactions from the Australian government was to talk to the police about opening another leak investigation.[2]

The need for a strong information security in newsrooms is real. And it isn't just for national security reporters anymore. Reporters who write about culture and lifestyle issues are doxxed on a daily basis. Television hosts are threatened and pursued by malicious trolls. Court reporters are hounded. Private companies, and not just governments, are taking it upon themselves to build an ever-expanding web of mass surveillance. The line between digital safety and physical safety is drawing ever closer.

And yet, almost a decade since the revelations about global surveillance revealed by Edward Snowden, many newsrooms still haven't figured out how to build effective strategies to combat these risks into their newsrooms. Mistakes are made. Journalists feel left in the dark, and frustrated at the lack of change.

Over the course of this study I've interviewed newsroom leaders, security experts and journalists around the world to try and find out what's working, what isn't and what we need to do to move the industry forward. Journalists from Italy, Norway, the United Kingdom, Botswana, the Philippines, the United States, France, India, Greece and the Netherlands participated in interviews.

The findings of those discussions are positive. They show real change is being made in pockets of the industry. Many of the organisations mentioned here deserve strong praise for their efforts, although all acknowledge that improvements could be made.

---

[2] Farrell P, Davidson H, Evershed N (2016). 'The Nauru Files: Cache of 2000 leaked reports reveal scale of abuse of children in Australian offshore detention,' *The Guardian* 10 August. Available at: https://www.theguardian.com/australia-news/2016/aug/10/the-nauru-files-2000-leaked-reports-reveal-scale-of-abuse-of-children-in-australian-offshore-detention (accessed on 27 June 2022)

This paper is an attempt to draw together the work of disparate organisations, often working in very different social, legal and technological environments, to provide some instructive guidance on how to build a strong culture to protect journalists and their sources from the many digital threats they face. The challenge they face, as one interview participant said, is "baking it into" their daily workflows in a way that journalists will find simple and straightforward.

This is not a definitive guide to information security practices in newsrooms. Other recent publications do that more comprehensively.[3] It is designed to be a roadmap for journalism institutions to help instil a strong infosec culture, and to consider some emerging threats and risks to how journalists operate.

[3] McGregor, S, 2021. *Information Security Essentials: A Guide for Reporters, Editors, and Newsroom Leaders*. Columbia University Press.

What's wrong with infosec in newsrooms?

Historically, the journalistic community has demonstrated a poor understanding and appreciation of the importance of strong information security skills and techniques. A 2014 Pew study found more than two thirds of respondent journalists took little or no steps to protect themselves using information security tools. Di Salvo (2022) describes it as an "ambivalent response".[4]

In a 2016 study, McGregor and Watkins conducted a series of interviews that identified that journalists' infosec approach ("mental mode") was rooted in a belief that precautions need not be taken unless the journalist was working in a highly sensitive area.[5] They note that journalists have "poor systems models" of digital communication technology, and that this mental mode may persist for as long as that remains.

The kinds of digital threats that may arise is also a constantly adapting area.
It requires frequent updates to ensure that risks are considered and responded to quickly. There has been some research into emerging threats, most notably from Anjuli R.K. Shere into the surveillance risks around "internet of things" devices.[6] Her study found that journalists in several different continents had a rudimentary level of understanding about the surveillance risks posed by connected devices such as smart watches, televisions and speakers – and an even more limited understanding of how to manage those risks. Part of the problem, according to one study, is that journalists have

[4] Di Salvo, P., 2022 Information security and journalism: Mapping a nascent research field. *Sociology Compass*, 16(3).
[5] McGregor S, Watkins E, 'Security by Obscurity: Journalists mental models of information security', *International Symposium on Online Journalism*, January 2016 Austin TX.
[6] Shere A, 2020. 'Security should be there by default': Investigating how journalists perceive and respond to risks from the Internet of Things. *IEEE European Symposium on Security and Privacy Workshops*

been unsuccessful in cultivating an effective "security mindset" that engages their interests and curiosity to engage with digital security protection measures.[7]

While many of these studies consider the attitudes and comprehension of journalists' understanding of information security risks, very few examine the culture of newsrooms. Perhaps the most advanced study in this area is Henrichsen's work into the role of the "information security champion" in newsrooms, and how key individuals operate within the nascent culture of a newsroom to instil and broaden knowledge.[8]

Henrichsen concludes that information security champions are necessary and important individuals in newsrooms that often have transient cultures. But they also raise the obvious question; what happens when the champions leave their newsrooms and go elsewhere? And is it possible to create an enduring information security culture in a newsroom setting? This is a key question this study sets out to answer.

Post Pegasus: has the game changed?

We've known for years that highly sophisticated intelligence agencies have the ability to penetrate individual devices in a manner that would reveal all of the contents of a phone. But private companies have increasingly been doing that work too, and selling their technology to less sophisticated nation states.

All of the journalists and newsroom leaders I interviewed felt one area of significant improvement in newsrooms had been the take-up of mobile encryption apps. Signal is widely considered to be the gold standard, and is used frequently for internal communications, as well as for establishing first contact with potential sources. Even five years ago, this was not the case.

---

[7] Tsui L and Lee F 2021 'How journalists understand the threats and opportunities of new technologies: A study of security mindsets and its implications for press freedom *Journalism* Vol 22(6) p 1339

[8] Henrichsen, J., 2021. Understanding Nascent Newsroom Security and Safety Cultures: The Emergence of the "Security Champion". *Journalism Practice*, pp.1-20.

Many interview participants agreed that the potential use of phone malware was an alarming development. At Norway's *VG*, reporters working on high-risk stories are allocated burner phones. They are instructed not to login to any services or make additional app downloads, and can only use it for basic encrypted communications.

At the end of the project, those burner phones are collected and tested forensically to determine if there are any traces of spyware on the phones.

To help in determining when a security attack has occurred, Amnesty International's Security Lab has built a command line tool that technically proficient users can access to analyse devices.[9] It requires a high enough understanding that it would be out of reach for many reporters to do on their own, and requires more technical support.

Less complex tools include the Iverify app that can undertake a basic sweep of an iPhone to determine if there's any evidence of an attack.[10] The app also has helpful checklists or guides to harden the phone against various forms of possible attacks.

The most prominent case study for understanding mobile device security comes from the team who undertook the journalism to expose the Pegasus spyware of the NSO group. *Forbidden Stories* worked with a consortium of newsrooms around the world to document many instances where journalists were targeted in ways that could have exposed their sources and themselves.

Laurent Richard is the founder and editor of *Forbidden Stories*. He founded the site six years ago, borne in part out of his earlier work travelling to countries with much less robust protections for freedom of the press than France.

---

[9] Amnesty International (2021) 'How to catch NSO Group's Pegasus'. *Amnesty International Ltd.* Available at:https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/ (Accessed on 27 June 2022)

[10] Iverify (2021) Iverify App. Available at: https://www.iverify.io/ (Accessed on 27 June 2022)

He brings a keen assessment of risk to every story; at the outset of all projects, his team develops a series of communication protocols for three key areas: communication between a source or sources and a journalist, communication between journalists in the organisation, and communication between other collaborators or participants in the editorial process.

“We try to build a plan about how to be robust as much as we can in our communication protocols; what kind of device; what do we say on that kind of device; what is the policy, how much do we delete, how often do we delete the messages; what can we say on this channel?”

The team is small – roughly 20 people – but since its inception it’s considered information security to be integral to what it does. And given the collaborative nature of the work they undertake, they are regularly working with potentially hundreds of journalists and editors around the world, requiring strict protocols for communication.

Richard is also a strong advocate of Tails, the incognito operating system. “It’s really a very comfortable ecosystem. It’s very easy to access, the concept itself is fantastic,” he said.

The group has developed a range of communication strategies to engage in safer encrypted communications for high-risk stories. One example Richard gives is of using the Signal encrypted messaging app, with an additional layer of protection by encrypting the text of those messages themselves using PGP.

What other lessons can be learnt from smaller outfits like Richard’s?

Infosec among innovators

Some of the most significant developments in newsroom information security over the past decade have been in smaller, more recently-formed digital startups. This is no accident. Many of these organisations have structures that are highly adaptive and responsive to changing digital environments. They have found ways to effectively incorporate strong infosec strategies into their workflows. Some have also pioneered new forms of collaborative journalism.

Their strength lies in understanding how to cultivate an effective security mindset for the journalists in their organisation. The risks they each face are particular and unique, and are informed by a complex interplay of legal and political considerations in their domestic environments. These accounts set out, in brief, some key features of the risks they face, and how they have approached overcoming them.

Case study 1: Fighting transnational corruption

When her friend and colleague Ján Kuciak and his fiancee Martina Kušnirová were murdered, Pavla Holcová was determined to turn her journalistic skills to the task of finding their killers.

“We thought we would tell this story about how you couldn’t kill the story by killing the journalist,” she said.

Holcová is the editor and founder of Investigate.cz, an investigative journalism website that has broken major stories in the Czech Republic. At the time of his murder, Kuciak had been working on a story about Marian Kocner, a Slovak businessman who had been a focus of Ján’s journalistic investigations.

One day Holcová received a call from a source. They told her they wanted to give her access to 70 terabytes of police files. She obtained them, and began working through the files.

But with such a vast body of information, working through it all was not easy. And there were obviously security risks. The risks around electronic government surveillance were significant and, given what had happened to her colleagues, could have quickly escalated into a physical security risk.

She turned to the OCCRP, a transnational investigative reporting outfit, for assistance. The organisation was founded by Drew Sullivan in 2006, dedicated to exposing crime and corruption. It has more than 170 staff that it employs directly. But it also works with dozens of partner organisations in Eastern Europe, Africa and the Pacific.

It's taken on an impressive list of powerful players in countries where there are serious threats to press freedom, working with journalists like Holcová all around the world.

Given the size of the organisation, it has a well-resourced information security team. Emma Prest is the chief information officer. Another employee provides training, and another provides risk assessments. Sullivan started the organisation with infosec front-of-mind, which she believes is a key factor in building a strong security culture.

"I think the security culture is pretty strong [...] because of the work we do; the part of the world we operate in, we've been under attack for quite a while," Prest said.

"It does mean that people are very aware of it. And so we have quite a good culture of people asking us, 'Hey, I need help'."

Onboarding is also key. Prest said all employees receive baseline training to bring them up to speed on encrypted email, encrypted apps. It's for everyone from new journalists to finance staff.

“A lot of people are actually quite freaked out at the beginning,” Prest said.

“We throw them in the deep end; we say you’re going to use Signal, you’re going to use Thunderbird, this is how you do encrypted storage, we’re going to set up 2FA on your work email and your personal email.”

Because habits change and threats evolve, refresher training is also held annually, in part to address any poor digital security habits they may have seen slipping into.

The organisation has a shortlist of “information champions” they’ve identified: people who are naturally interested in these issues, and who are good at engaging with the tech and giving feedback on what works and what doesn’t.

This approach to training and managing risks made it easier to respond to high-risk scenarios that reporters like Holcová have experienced. Sullivan assigned a team to assist in modelling the threats. They created a safe room to access the data, with strict conditions on how it could be accessed and by whom. Contact between participants was largely conducted via the encrypted messaging app, Signal.

Holcová said she believes it was more beneficial having an independent, outside perspective on the security practices they deploy in the newsroom.

“What I’ve learnt is that if you are dealing with sensitive information, you tend to underestimate or overestimate the risk. You need that person to talk to. You really need to take a step back and look at a sensitive project,” she said.

The impact of the story has been seismic: it was a major contributor in the downfall of the Slozak government. Kocner was charged and convicted for the murder of Kuciak, but was acquitted in 2021. A retrial is under way.

Case study 2: Digital safety is changing – and so are the reporters at risk

Information security is no longer the sole dominion of a handful of investigative reporters and conflict reporters. Increasingly, there are newer threats to a much larger pool of journalists and editors. Mark Schoofs, who was the editor of BuzzFeed News from 2020 to 2022, said that while the organisation has always prioritised source protection for investigative reporters working on complex and high risk stories, it became increasingly concerned with managing the personal risks to all journalists' safety from online abuse.

"We find that a lot of people who write about [celebrities], or who write about social media influencers, suffer extraordinary harassment," he said.

"They just get swarmed with hate and abuse, doxxing, and all of that. So, you know, it used to be like, 'Oh, well, its those journalists who do hardcore stuff that need the security'. No: everybody needs it."

At times, Schoofs said, responses are so extreme they can escalate into threats to their personal safety.

This particular information security threat is impacting news organisations around the world. BuzzFeed's response was to systemise a response; it rolled out extensive training that helped their staff to audit and harden their social media presences. The purpose of this was to limit their potential exposure – and the exposure of their personal networks – in the event of a backlash.

The training is extensive, and takes reporters through steps to harden their Facebook, Twitter and other social media profiles. In the event of a specific threat, the information security team will step in to provide additional advice, review their social media accounts, and even take over public accounts. A key objective is to create largely

separate public and private digital presences, so reporters can step away from their public profiles when necessary and limit the risk to their personal networks.

The company also offers a paid service to staff that scours data broker websites for information about their journalists, and makes data removal requests. This is to reduce the risk of doxxing, which can lead to a reporter becoming physically compromised.

Schoofs said the company has embedded information security into its workflow by constantly talking about it, and talking about best practices. Security isn't an abstract topic to be palmed off through once-off training.

"It can't just be 'you take some courses and you know how to deal with it'," he said. "There have to be [ongoing] discussions with your editor and the security team."

Case study 3: Lighthouse searches for high-tech and low-tech solutions

Lighthouse Investigations is a small non-profit news organisation based in the Netherlands. It has broken significant stories about migration and arms exports across Europe and elsewhere, and partners with other news organisations on a regular basis.

Managing director Daniel Howden told me his newsroom is now contemplating high-tech threats that two years ago seemed in the realm of science fiction.

"Things like faraday pouches are sitting on the office desk," he said. A faraday pouch is a tool that looks like a small pouch for a phone, but is actually designed to muffle and mute all electronic and network connections to a digital device. For Howden and his team, tools like this have become an unexpected reality.

The newsroom has a headcount of less than 20 people and, because of its size, doesn't have a dedicated staff member who specialises in only information security management. But it keeps security issues front of mind. Howden said the organisation has turned its attention to contemplating the increasingly real risk of spyware attacks.

"We've had to basically familiarise ourselves with the available tools for doing device scanning and to think seriously about the manufacturers of devices, junking all the ones with vulnerabilities," he said.

Not every investigation will carry that level of risk. Senior editors determine whether or not they need to conduct a risk assessment as a starting point for all stories.

"We calculate our risk profile or threat profile. Once it reaches the stage where you assume you could get targeted, protocols become hugely more complicated," he said.

Howden is cautious about being too prescriptive with tools and techniques. He argues that low-tech solutions are likely to become increasingly used.

"If it comes down to source protection, [it] will have to move to low-tech: having burner devices, in-person meetings, keeping handwritten notes and then only sharing very specific things. It's simple enough to set up your own code for some basic communications. [Infosec] doesn't have to be too elaborate to make it a significant challenge for people outside the organisation."

Training is something the organisation is still working on, as well as standardising approaches. "That's something we definitely need to become better at. What we're trying to do at the moment is come up with a better defined onboarding process for launching investigations," Howden said. "So there are a series of repeatable steps that we follow to launch most investigations, make sure there's certain documentation in place, and it's clear to everyone what steps need to be taken for secure communications about the investigations and storing of the findings as we go."

Case study 4: Serbian journalists under attack

Serbian news outfit KRIK is getting close to the point of having more lawsuits filed against it than staff members.

“The situation is bad, and unfortunately it’s getting worse and worse by day,” said Bojana Jovanovic, an investigative journalist and the deputy editor of KRIK.

She and her colleagues have found themselves repeatedly targeted in aggressive smear campaigns led by the government. Most recently, they were accused of being linked to a specific organised crime group.

“They put us in danger because [that] organised crime group was in a war with another organised crime group,” she said. “They are putting targets on our heads.”

Their organisation has a high level of risk. Jovanovic said their office and some staff members are believed to be under high levels of physical and electronic surveillance. There have been break-ins at the homes of reporters. In one instance a staff member was placed under physical surveillance and photographed speaking with a contact. The image was then published in another news outlet.

“The government is now trying to scare our sources in order to send a message,” Jovanovic said.

As a consequence of this, they have strict communication protocols with sources and amongst themselves. They communicate largely via Signal or PGP email. Discussions of sensitive stories are rarely held in their offices, and instead are held at another location, where phones and other electronic devices are not allowed.

KRIK also works with the OCCRP on larger and more complex stories. Jovanovic said that the most important part of the process is to communicate clearly with their journalists on how to mitigate risks at the very start of the story process.

“We need to explain why it is sensitive, how to act, how to communicate. It’s really important to give a headstart to all journalists so they know how to process and how to work on the story,” she said.

Case study 5: Infosec for sources

One of the obvious challenges when journalists are dealing with higher risk stories is communicating with sources. Once first contact has been established with a potential whistleblower, the question of where and how to take the conversation requires a high level of understanding of information security practices.

It requires a detailed understanding of conventional and digital surveillance risks. It also requires having frank discussions with sources about how you will communicate with them.

Alvin Ntibinyane is the founder of the INK Centre in Botswana, which undertakes investigative reporting on government and private corruption. In 2018, his team went on a major push to ensure their sources were using encrypted messaging apps. “What we did was [...] offer our sources basic training with Signal,” he said. “It has worked. They send documents using Signal.”

That task can at times be challenging; not all sources have the same level of technical skills. “When we did one story in 2017 we had one guy trying to use Signal. He had a smartphone but struggled with it. We had to spend hours with him,” Ntibinyane said.

The challenges Ntibinyane outlines around encouraging safe communication were echoed by other interview participants. And, while larger newsrooms have also adopted clear communication postures by outlining a range of first contact strategies, sources don't always listen to the advice they're given.

"Infosec is a two-way street," Schoofs said. "You and your organisation can be great about it, but you're only one half of the equation." He gives the hypothetical example of a reporter speaking with a confidential source. The journalist takes all necessary precautions, including setting deleting messages on their encrypted messaging chat. But the source decides not to.

"Your source, for whatever reason, decides that they're to go with whatever they're familiar with or however they wish to communicate even if that method of communication is less secure. And we don't really have a good answer for that. You can't force people to do something different."

Schoofs also raises another possible danger; if a reporter coaches their source on precisely what steps to take to encrypt their communications, it could also put them at risk depending on the legal environment.

"If you are taking great pains to talk to a source and explain to a source exactly how to use Signal and avoid the government, you may have entered into a conspiracy with that source to illegally obtain classified information," he said.

While the precise operation of conspiracy and forms of accessorial liability vary significantly in different jurisdictions, legal practitioners interviewed in a number of common law systems like Australia and the United Kingdom acknowledged this appeared to be a potential risk.

In the United States, this is now more than just a theoretical possibility: Schoofs points to some of the charges in the indictment of Julian Assange. "Some of those acts in

which he's charged are very hard to distinguish from what journalists do everyday," he said. "You could imagine journalists at the *Washington Post* or the ABC or whatever doing exactly those things."

Schoofs offers a practical solution: he wouldn't want his reporters walking a source through every step of the way, but "maybe send the source to a website that explains how to use Signal? Put a little bit of distance between yourself and the source to deal with this grey area of American law".

Lessons from small newsrooms

All of these newsrooms have made important strides in integrating a strong security culture into their workflows; all of them acknowledge they could still do more.

While they work in vastly different environments, some common themes and strategies emerge from them.

The first is having strong leadership that instils infosec culture from the outset. Each of the organisations has senior editorial leaders that recognise the importance of information security risks and take steps to establish protocols to manage them in their editorial workflows.

The second is ensuring that information security risks are factored into the editorial process as the story develops. This is consistent with McGregor's view that these risks need to be front-of-mind for all journalists and editors, in much the same way as they know when a story needs to be checked by the legal team.[11] Many of these organisations also point to the fear of reputational damage they may suffer if they don't act appropriately from the early stages of a story. In McGregor's words: "Every reporter, editor, and newsroom leader needs to understand the foundations of information security if they hope to avoid the industry's cardinal sins: outing a source and becoming the story."

The third is developing workflows that are easy for journalists to manage, and avoiding unnecessarily complex tools. All advocated the use of Signal for internal communications. Each organisation also offered a range of encrypted tools for first contact, including Signal, Securedrop and, in some circumstances, a Protonmail email

[11] McGregor, S., 2021. *Information Security Essentials: A Guide for Reporters, Editors, and Newsroom Leaders*. Columbia University Press, 2.

address. The more complex the tools, the less likely journalists – as well as sources – are to use them, and the more likely risks will be taken.

The fourth is considering the potential interplay between information security and physical security. Harm minimisation strategies – like those deployed by BuzzFeed to harden social media presences – are a valuable tool in diminishing the impact of online attacks, and decreasing the risk of a physical attack. Mapping out key and emerging risks for staff and how they could lead to physical attacks is a crucial part of any assessment of information security risks.

Finally, each of these organisations demonstrated a strong security mindset. Senior leaders had a clear understanding of risks, and these were communicated across the editorial workflow, and among all staff members. This mindset informed their approach to executing complex journalistic activities in a way that minimised potential harm for them and their sources.

Many of the organisations discussed above are relatively new, and have small teams that can adapt to threat with more agility. Their experiences are useful in providing some strategies and instructive guidance to larger, older newsrooms that are still coming to grips with how to embed strong infosec cultures.

What tools should journalists actually be learning?

Everyone I interviewed said it was impossible to be too prescriptive in explaining exactly what tools journalists need. The risks and threats for different journalists operating in different environments will shape the responses required. As a result, discussions of information security for journalists tend towards abstractions that are of little use to practitioners.

For this reason, I will set out a brief snapshot of some common tools referenced by interview subjects that are broadly in use. Before considering their use, consult more definitive resources that are regularly updated to ensure that no vulnerabilities have emerged.[12]

- Signal, mentioned extensively above, is by far the most ubiquitous tool referenced by interview subjects. It is regularly used as a first contact tool, and the widespread take up of the app and ease of use has made it a strong first choice for many journalists. It is also used frequently for communication within newsrooms. Some journalists also used Signal in more sophisticated ways, such as communicating via iPods while using the app.
- Some participants explained that due to the rise in the use of Signal, the use of PGP email encryption as a first contact tool and for internal communication had diminished. But others also said there was a renewed use and interest in PGP due to an increase in concerns over mobile phone spyware. Others still reported that PGP was used for other purposes such as file encryption.
- Similarly, while tools like Off the Record (OTR) messaging were previously common five to ten years ago, they appear to be in less frequent use due to the ubiquity of Signal.
- Some interviewees did use tools like Onionshare for receiving files anonymously from sources, but this use had also been diminished by the now broad take up of Securedrop in many newsrooms or file transfers via Signal.
- The Tails operating system, which has been in use for a long time and is endorsed by many security practitioners, has gained increasing prominence and

[12] Electronic Frontier Foundation (2021) *Surveillance Self Defence* Available at: https://ssd.eff.org/en (accessed 5 June 2022); Freedom of the Press Foundation (2021) *Guides and Training* Available at: https://freedom.press/training/ (accessed 5 June 2022).

use. Some interview practitioners believed that the operating system has vastly improved in its day to day usefulness to a decade earlier.

- Two noteworthy new tools are worth pointing to; the first is the Qubes operating system. The technical threshold is likely to be a challenge. Few interview subjects were aware of current practitioners that were using Qubes in their daily workflow, or even for more sensitive one off projects.
- A further tool of note is DangerZone, developed by Micah Lee.[13] It allows users to convert potentially malicious files that may have malware into safe files. Given that many attacks on journalists are through malicious email or other types of files, this tool may prove useful for journalists seeking a quick sandbox solution that doesn't not involve using a separate device.

What was perhaps surprising from these interviews is how few new tools are in use. Instead, the uses of existing digital tools have changed and adapted over time. In Natali's view, this is a welcome development.

"We need to consolidate what we have in a healthy way," he said, noting his hope that over time we actually have fewer tools that are part of a more secure fabric of digital security.

[13] Micah Lee (2021) *Dangerzone.* Available at: https://dangerzone.rocks/ (Accessed 5 June 2022)

How to turn a big ship

Effecting change in a big newsroom is a notoriously difficult task. For larger legacy organisations, it can be cumbersome and difficult to change course and adopt proactive policies around information security.

They may have highly skilled people who have the knowledge required, but they are unable to integrate them effectively. When new systems or processes are needed, it can also be difficult to filter them through the organisation:

"The separation of responsibilities is already enshrined in org charts and budget lines, and the question of where information security should sit within the organisation is controversial," McGregor observed.[14]

Lucy Kueng's analysis of shifting newsrooms to digital practices provides a valuable template for changemaking in newsrooms, and she summarises the dilemma in this way: "Knowing what to do does not mean that you will be able to do it."[15]

She identified several core features for change. The value of leadership buy-in is critical. If the top leader isn't driving transformation and setting norms for how people interact, she writes, "then everyone else can down their change tools".

Kueng also notes that newsrooms have historically had a weak feedback culture.[16] Working out how and why things should be done differently has never been clear. Putting in place a strong system for reflection on information security cultures at regular intervals will also help diminish these issues.

---

[14] McGregor, S., 2021. *Information Security Essentials: A Guide for Reporters, Editors, and Newsroom Leaders*. Columbia University Press, 159.
[15] Kueng, L 2020 *Hearts and Minds: Harnessing Leadership, Culture, and Talent to Really Go Digital* Reuters Institute for the Study of Journalism, xi.
[16] Kueng, L 2020 *Hearts and Minds: Harnessing Leadership, Culture, and Talent to Really Go Digital* Reuters Institute for the Study of Journalism, 13.

McGregor agrees that buy-in is critical from senior leadership:"Ultimately, your information security team's work can only be as robust as the engagement they have from the broader organisation. You must think strategically about how you will raise awareness of — and help generate buy-in for — the work of your information security team."[17]

Simply raising awareness internally about the activities of information security teams can bolster engagement and buy-in from other parts of the organisation. Written guides, videos and in-person or online training at regular intervals can also improve engagement and build knowledge.

Appoint a dedicated security champion

An important feature that some larger newsrooms have now adopted is a specific role dedicated to editorial information security needs. These champions are more than just ad hoc experts; they are specialised and dedicated officers who take on the role in a formal capacity.

Most interview participants in this study who had experience working in larger newsrooms agreed there should be a dedicated officer to provide advice on information security issues.

This individual would be consulted at several stages during the production process: at the start, to assess risk and outline tools or strategies, during the journalistic process as new challenges or unforeseen events arose, and in the immediate pre- and post-publication stage to assess ultimate risks.

They may also engage in broader reviews of information security awareness, and provide training to staff at key intervals, such as during the onboarding process.

[17] McGregor, S., 2021. *Information Security Essentials: A Guide for Reporters, Editors, and Newsroom Leaders*. Columbia University Press, 159.

BuzzFeed's Schoofs said the changing nature of digital safety makes a strong case for a dedicated role. "Just to keep track of the digital stuff is a huge effort", he said.

But he remains firm that this role should not be a decision-making one on key editorial issues. "Security people are like lawyers, they are advising. But ultimately the editor or the editor-in-chief should make the decision."

Where my interviewees' opinions bifurcate was in determining what that role should look like, and how it should interact with the different parts of the organisation. Some suggested the role should be largely integrated with physical security officers, who assist staff deploying to conflict regions. Others saw the role as more embedded in the newsroom itself.

One model that has been deployed in big news organisations involves embedding the role within business or enterprise technology and IT teams. But there are also some challenges with this model.

"I think it made it harder to develop relationships with some of the desks in the newsroom as a part of that," Kristen Larson Kozinski said. She was the information security trainer manager at the *New York Times* from May 2018 to March 2022, and now works in a similar role at Yahoo. She said one of the biggest challenges she found was coming in as an outsider to the newsroom."Newsrooms are relationship-based organisations and groups," she said.

"You need to start making connections with the heads of desks, the leadership, and the people who aren't necessarily in leadership, but are seasoned and have been there for a while who have influence outside of just their job title."

Because the type of role is so new, the most likely staff are going to come from a background working with tech companies. That can also lead to culture clashes. Traditional security roles may not always be the best fit for a news organisation.[18]

Trying to find ways to work with journalists to find solutions to their workflow problems and understanding what they need is also vital. The best people for that role will be individuals who are genuinely interested in journalism.

“It's important to listen, ask lots of questions, understand what the general norms present in that newsroom are and how you can work around them and develop with them,” she said.

Kozinski believes one potentially more effective model could be an editorial trainer who is embedded in the newsroom but still has links to the business or enterprise side of the organisation. “I feel like an ideal situation, which I haven't seen, would be a training team that would have two managers: [a manager] who’s in the newsroom and able to help them build those relationships and connections and direct the path of different projects, and [a manager] in the enterprise part of the company because I do think they go hand-in- hand.”

Runa Sandvik, who worked at *NYT* as senior director of information security from March 2016 to October 2019, takes the view that the best possible place for this role is within the reporting structure of the enterprise or business side, but with the editorial security officer physically sitting in the newsroom. The main benefit to this approach, she said, is that many of the solutions that journalists will need – such as software requests –will need to be implemented by the IT Infrastructure side.

[18] McGregor, S., 2021. *Information Security Essentials: A Guide for Reporters, Editors, and Newsroom Leaders*. Columbia University Press, 160.

This approach would also minimise the risk of "shadow IT", where reporters workaround prohibitive IT policies in ways that limit the visibility for security staff about what tools journalists are accessing.

One newsroom that thinks they've cracked the code is Norwegian news outlet, *Verdens Gang* (VG). Einar Otto Stangvik is the newly appointed director of editorial security at *VG*. His role was developed after several earlier attempts to improve information security. Stangkik, who was initially brought on as a developer in 2014 and has also worked as a journalist and researcher, was involved in several committees and groups that sought to make changes. But he kept running into the same problem: "Things stopped once we left those meeting rooms," Stangkik said. "Nobody had been able to take it much further because there'd been no-one there with a mandate, no-one there with an actual responsibility for the newsroom."

VG's holding company Schibsted does have its own well-resourced security team, and it conducts the sort of training you would see across all large corporations: phishing mitigation, two-factor authentication instructions and emphasising strong passwords. But Stangvik said there's too much distance between that and what a lot of journalists actually do. "They have to provide a one-size-fits-all security for different companies and that doesn't work too well with journalism," he said.

Stangvik believes in making infosec as accessible as possible. Rather than leaving time-poor reporters with a massive document with hundreds of pages to digest, he's developed a basic security poster to help outline the different levels of possible risks and what steps should be taken. In cases with more elevated risks, staff are encouraged to contact him. In cases where the risks are high, they are required to speak with him at the outset of their project or investigation. From that point, much of the work that Stangvik does will be in person or communicating directly with journalists.

When Stangvik's role was developed, there was plenty of discussion around where exactly he should be located. Should he be part of the security team? Should he be his own department head, with his own staff? Ultimately, they adopted what he considers to be a hybrid model: he sits in editorial development in the newsroom, reporting to the editor-in-chief with the title of head of the editorial security department. He has agency and autonomy over who he assists in the newsroom and the kind of assistance he provides. His ties to the newsroom, he said, have been a strong asset.

Use expert external training

In many newsrooms around the world, and many companies more broadly, there's been a painful trend towards automated online training "modules" that all staff are required to complete. This kind of training was almost universally renounced by interview participants in the area of information security training for journalists. This is because infosec uses and applications for journalists are often far more specialised than any broad based training can cater to.

Fabio Natali is not a journalist, but found himself increasingly drawn to the work they do after attending digital security events known as Cryptoparties that put him in closer contact with journalists and other like-minded digital rights people.

He's since become involved in running training for the Centre for Investigative Journalism in the UK, which developed a program with the assistance of the Freedom of the Press Foundation. The development was rooted in two key objectives: the first was that it should encourage a mindset shift and not just teach a set of steps, the second was that it should introduce the concept of threat modelling, and how to gauge and understand risks.

“The way we teach is hands-on”, he said. “We drill down into specific examples and scenarios.” The training gradually progresses into nuance and specificity, exploring the advanced use of Signal, and ending in an introduction to Tails, a portable OS.

Journalists need a network of credible experts they can approach for advice, he said. And one-to-one training is critical to ensure journalists can ask questions that are specific to their needs.

Declutter internal training

Many interview participants advocated for a broad-based “baseline” training for all employees. The OCCRP has developed this as part of its onboarding process. Sandvik also agreed that a form of baseline training should be provided: covering security basics such as Two Factor Authentication and encouraging the use of password managers.

Stangvik’s approach to more advanced training at *VG* is to deliver it on the job, when journalists approach him during the editorial process. “My approach is to establish specific setups for specific stories. Once we’ve done this over and over, the same people have done the same setups five or 10 times, then you’ve effectively trained them to use these tools in practical scenarios,” he said.

He believes the process should be peer-led: “It’s much more helpful to have a journalist who has had Pegasus put on their phone talking through what that feels like to help understand those risks,” he said. “That’s more beneficial to understanding what security and risk means than just sending out an email.”

A security culture checklist

Newsrooms often seek practical guidance and instruction on how to improve their processes quickly and efficiently. Based on the above discussion points and interviews with stakeholders, key patterns emerge that show what goes into making a strong information security working culture. Any newsroom seeking to take a step back and critically examine its own practices may wish to consider the following checklist of working practices:

- Do editorial staff exhibit a strong "security mindset", where they are capable of identifying if and when information security risks may arise?
- Is information security risk assessment factored into the editorial and production process, similar to the way legal risks are assessed?
- Does the newsroom have a dedicated employee who is tasked with managing information security issues? If it doesn't, is there a clear accountability for these functions held by another officer?
- Is a form of baseline training provided that helps newsroom staff develop a "security mindset" and provide some key baseline skills?
- Is there more advanced training on offer, and is it accessible to staff?
- Does newsroom management endorse and buy-in to the promotion of information security management in the newsroom?

Conclusion

Every day, all over the world, people reach out to journalists asking them for help.

Some of those people are taking a chance when they do this: risking their lives, their jobs and their security to communicate something they believe the public needs to know about.

In doing so, they put their trust in us – collectively – to do all we can to protect them. Having a strong culture of information security helps ensure their trust is not misplaced.

As the range of threats grows in intensity and endangers journalists themselves, having that strong culture will not only help sources, but journalists too.

Newsroom leaders can be doing more. This paper has outlined key observations from a range of journalists engaging with new ways of thinking about information security risks. While not every approach will work in every newsroom, taking a step back and examining work practices, scrutinising organisational structure, and thinking about where information security fits into it, can serve to create an enduring culture that protects journalists and their sources.