Wake up digital forensics' community and help combating ransomware

Jan Huck
Institute of Information Systems, University of Liechtenstein, Liechtenstein

Frank Breitinger[‡]
School of Criminal Justice, University of Lausanne, Switzerland

***Abstract*—To combat ransomware, organizations, literature, and research efforts focus on technical measures and neglect procedural countermeasures (e.g., incident response plan, business continuity plan, and communication plan). We argue that detailed case studies and best practices need to be shared to allow companies to adapt their strategies to be better prepared.**

PREFACE For this work, we presume two communities dealing with ransomware: the security community (SC) and the digital forensics community (DFC). While there is beyond all doubt overlap[1] between these communities, we argue that both disciplines have different strengths that can be helpful to combat ransomware. For instance, SC often targets the prevention and detection of ransomware in comparison to DFC who concentrates on investigation, incident response, business continuity or backups and recovery. We argue that especially those topics under the DFC umbrella benefit significantly from best practices, case studies and examples.

[‡]Most of the work was completed when still being affiliated with his previous institution the University of Liechtenstein.

[1]A common overlap is reverse engineering which may be relevant for both communities.

Introduction

On July 23^{rd} 2020, Garmin Ltd. became the victim of a major ransomware attack. While there are many attacks, this one revealed three interesting lessons learned: First, ransomware attacks cannot always be prevented regardless of the industry (e.g., in this case a large company in the tech sector). Consequently (second), a backup alone is insufficient. To minimize loss and not pay the ransom, sophisticated recovery strategies which include a solid backup plan are essential (in this case Garmin paid a multi-million-dollar ransom). Third, a good incident response strategy including a communication strategy on how to handle the incident is important. Many users

complained about the limited communication [1][2] resulting in disgruntled customers.

Unsurprisingly, ransomware countermeasure recommendations such as from [2], [3] or [4] underline the importance of the previously mentioned aspects and stress incident response strategies as well as sophisticated backup and recovery strategies (a summary of the different taxonomies is listed in Table 1). In contrast, when looking into ransomware literature, one sees that the number of articles addressing those aspects is limited. On the other hand, there is a significant amount of research / literature in the areas of ransomware prevention and detection (domains we consider falling under SC). Consequently, in this article we are interested in understanding the following questions

- Q1 Given ransomware countermeasures recommendations, which measures are actually implemented by businesses and which are not?
- Q2 How do available online resources compare to given ransomware countermeasure recommendations?
- Q3 How can the digital forensics community help to combat ransomware?

To answer these questions, we conducted a qualitative study by interviewing 10 experts (eight IT departments of companies and two cybersecurity professionals) in the extended Rhine valley (Switzerland / Liechtenstein) as well as conducted a literature review. In summary, results show that:

- Most research and companies focus on prevention, detection, and prediction.
- These are also the areas most companies invest in (i.e., companies invest in technical measures and network security).
- Companies and research neglect incident response strategies, user security education, security policies and awareness of management.
- Case studies / best practices often do not provide sufficient detail while research conducted in the DFC area is often too abstract (not applicable by industry).

[2]Many of these comments were found on Twitter and included statements such as crisis management is near non-existent or non-existent communication and woefully weak FAQ (more details see [1]).

Distinction

Parts of this work have been published in the Master thesis by [5]. The thesis focused on comparing companies' implemented ransomware strategies and given best practice. In comparison, for this article we are less interested in general aspect but those related to digital forensics. Thus, this work utilizes results from the thesis but has a significantly different focus and outcome.

Limitations

The interviews were conducted in a specific region in Europe, which may have an impact on the results as other regions may apply different practices. Furthermore, the number of conducted interviews is small and may not properly reflect the current situation. Similarly, the same applies to the selection of companies, as these were chosen from different sectors and sizes. The second part of this work is based on the manual search and analysis of research articles, white papers, blog entries and more, which allows for the possibility of human errors such as missing literature or neglecting relevant sources. To counteract this, we have applied the four eyes principle. Regardless these limitations, we believe that this article includes relevant aspect fostering the discussion in the digital forensics' community.

Ransomware countermeasure taxonomy

Literature research revealed that a tendency exists to reduce ransomware protection to a technical level, focusing on preventive and detective measures [6]. However, international standards such as the ISO/IEC 27000-series, agencies such as the Bundesamt für Sicherheit in der Informationstechnik (BSI) in Germany, or cybersecurity research in general recommend a comprehensive approach which includes multiple factors next to technical ones. For example, [7] have suggested to include human and organizational aspects because vulnerabilities in these areas cannot be fixed by technical means. Countermeasures and recommendations have been published to help organizations to be prepared for ransomware attacks. For this work, we utilized a ransomware countermeasure taxonomy which follows an all-around approach towards ransomware protection. It is based on [6] but was redefined by us considering other relevant literature, e.g., [8] or [9].

The taxonomy is shown in Table 1 and consists of six dimensions with multiple sub-categories.

Table 1. Adjusted ransomware countermeasure taxonomy.

Dimensions	Sub-dimensions
User security education	Continuous Face-to-face Relevant content Exercises On all levels Encourage to read documents
Technical measures	E-mail hygiene Upgrade management Monitoring Backups and recovery Web protection Whitelisting
Network security	Network infrastructure Access control management RDP maintenance
Security policies	Report suspicious activities Shut down devices Agreements with partners Password management Devices for business-only use Deinstall unused software Avoid using freeware
Incident response strategy	Incident response plan Business continuity plan Communication plan
Management	Drive cybersecurity Communicate importance Security and IT knowledge Cultivate culture and attitude Provide funding

The following observations were made:

- Nearly all analyzed sources stress the importance of *user security education* to raise awareness. An important aspect was that training should not only focus on phishing but also include aspects such as to report suspicious behavior immediately.
- Even if an all-around approach is favored, *technical measures* and *network security* are still an important basis. While many technical solutions are sophisticated, [10] argues that "recovery [is] a vital component of every organisation's cybersecurity strategy. Yet current approaches are manual, cumbersome and inefficient – or else costly and time-consuming to build. Recovery is just not thought of as a solid last line of defence".
- Employees must be guided by *security policies*. Therefore, it must be ensured that they are up-to-date and are followed which is often not the case.
- The *incident response strategy* contains plans for the case that a company is infected. The proper preparation and training can improve the ability to react in an emergency and thus give the company the ability to gain valuable time as well as recover all data.
- *Management* is the enabler of change that can drive transformation within a company. Mid-level management must implement appropriate security measures and communicate the importance of them. To be able to do that, basic knowledge in cybersecurity and IT is needed. At the same time, the top-management must push forward a beneficial company culture and provide funding.

Note, that this is not an ordered list or ranking. While we searched in literature which ransomware countermeasures are most important, sources either do not rank their measures at all, or the ranking differs between sources. As there is no clear overlapping, we assume that no real ranking between ransomware countermeasures exists, but that all are of similar importance.

Interview methodology and findings

To get an understanding of implemented countermeasures, we started by doing a qualitative survey (interviews). We decided for this approach as almost no qualitative surveys on ransomware have been conducted so far. One exception is the already mentioned article by [6] in which the authors examine twenty-six ransomware incidents via interviews to design a countermeasures taxonomy. On the other hand, several quantitative surveys (questionnaires) have been conducted to find out how companies perceive the threat of ransomware, if they have been infected, and if yes, how they were attacked and what the aftermath of the infection was. These studies were either conducted by public agencies, cybersecurity vendors or research organizations.

Interview design and methodology

The interviews were semi-structured, meaning that they followed a predefined protocol, but allowed for follow-up questions and discussions. This qualitative approach was utilized because it

boasts the advantage of exploring why a phenomenon occurs as it does.

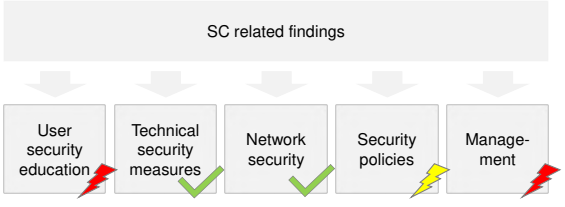
Target group
The ten interviews were conducted in the extended Rhine valley: eight with companies, and two with cybersecurity professionals. This split was done to have a clear focus on IT employees while having the possibility to discuss results with experts. Respondents from the companies were either the head of IT, the person in charge of cybersecurity, or in one case an employee with thirteen years of experience inside the company's IT department. The companies were selected from eight different industries, had between 80 and 1200 employees and were from public and private sector. The second group of interview partners consisted of cybersecurity professionals with strong connections to businesses in the target area.

Interview findings

The upcoming three sections discuss: SC related findings, DFC related findings and successful ransomware attacks.

SC related findings All interviewees agree that ransomware is a high to very high (being the most prominent current cybersecurity threat) threat for all companies from all sectors. Interestingly, five companies see themselves well prepared in general against a ransomware attack, while three reported that they are technically well-prepared, but need for improvement in some areas, for example, in procedural and managerial aspects. A summary of the results is depicted in Fig. 1 Details are discussed in the subsequent paragraphs.

Figure 1. Security Community (SC) related findings (green indicates 'interviewees reported sophisticated measures', yellow indicates 'average measures' and red indicates 'weak/no measures')



User security education varies significantly between the interviewed organizations. We classify four strategies satisfactory, i.e., they are at least continuous, face-to-face, take staff from all levels into account, and include additional awareness campaigns like exercises. On the other hand, the remaining four show insufficient training, e.g., one company only sends out newsletters via e-mail or intranet to inform about threats, one conducted a workshop just once because of an external analysis, one utilizes e-learning only once during the onboarding process, and one only invests in training IT staff.

All companies believe that their *technical security measures* are good or even excellent. For e-mail hygiene (including scanning and filtering), centralized upgrade management, advanced monitoring & detection tools, and content filters nearly all companies state that their measures are state-of-the-art. Furthermore, interviewees pointed out some additional measures such as advertisement blockers, SSL interception or application whitelisting approaches.

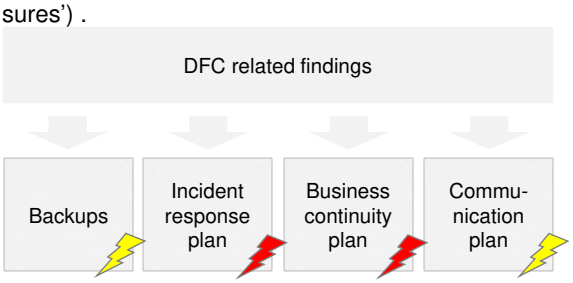
With respect to *network security*, all companies describe their network as segregated or even heavily segregated, state that they have a separate guest WLAN, and that external access is only possible via Citrix or VPN, or in the case of one organization with specialized technology which records what the user is doing. Six companies report that only business devices are allowed on internal network.

In terms of *security policies*, one company states that they have an IT manual, development guidelines, IT baseline protection, and security by design in project management. But they did not go further into detail. All other companies state that they have IT guidelines and follow the least privilege principle. All but one forbid private devices. Furthermore, three report that business-only policies exist.

Only three companies believe that the *management* has satisfying knowledge of IT security and perceives it as an essential topic. This can be attributed to their business model focus or to previous attacks. The remaining companies declare that the management does not care about IT at all, sees cybersecurity as a pure IT topic, or only grants monetary resources for technical measures.

DFC related findings Most interviewees agree that a backup strategy and an incident response strategy, including an incident response plan (IRP), business continuity plan (BCP), and communication plan, are important measures against ransomware. A summary of our results is depicted in Fig. 2.

Figure 2. Digital forensics community (DFC) related findings (yellow indicates that 'interviewees reported average measures' and red indicates 'weak/no measures') .



All organizations report that they have a decent backup strategy in place, including in some cases redundant backups stored in different locations in multiple versions. But upon further inquiry it became apparent that their strategies have flaws. The biggest weakness identified is that only three organizations conduct offline backups. One of them also revealed that they think about replacing them with online backups. As reason for not storing the backups offline, interviewees argued that the volume of their data is too big and that available technologies, for example tape, are too slow to fulfill their needs. In contrast, literature and both interviewed experts stressed that it is essential to have backups that are not connected to the company's network. Additionally, having a backup alone may not be sufficient if it takes 'long' to revert systems (e.g., if stored on tape) or if the recovery process is never tested / practiced.

Only two companies report that they have a comprehensive *incident response plan (IRP)* and that they have a contract with an external partner for emergencies. Moreover, two organizations have a basic plan, and one company has one which revealed flaws upon investigation, as it only covers the company's main site, but not remote offices that are connected to the same network. All in all, only two IRPs can be classified as satisfactory.

For the *business continuity plan (BCP)*, three companies state that they have a functioning BCP. Two reveal that they have a BCP but that experience has demonstrated that it does not work; the company could just reach a fraction of the normal throughput. Additionally, one of the organizations without a BCP remarked that the coronavirus demonstrated to them that chaos emerges as soon as there is a deviation from regular operations.

A *communication plan* was found in six companies. Five of them are more developed, while one is basic and just states that management needs to be informed[3].

Successful ransomware attacks Four of the companies experienced a ransomware attack. One of them had a minor, two a medium, and one a substantial impact (presented in this order)[4].

Attack 1 (minor, 2020)
A zero-day exploit allowed compromising Citrix NetScaler, the system that handles the login of users from outside the network. The IT department noticed a heightened load via monitoring tools and since no incident response strategy was previously defined, they acted based on ad hoc decisions. They manually investigated the system and found unknown processes. They suspected that they are related to ransomware (no 100% certainty), and due to recent media coverage about the exploit, they reacted quickly. They reset the system and restored a backup, which stopped the attack from advancing into the network at the outermost layer. The attack could be averted with almost no damage.

Attack 2 (medium, 2016)
A legacy device, which cannot be updated due to special software requirements, was infected, presumably through exploiting the old operating system. An employee noticed that he cannot access the data anymore and informed the IT department, which followed their IRP immediately. In less than 30 minutes after the notification, the IT replaced the infected device with a backup machine, which they kept ready for this critical production

[3]The interviewee was not sure, if a more detailed communication plan for the management exists.

[4]Since the original goal of the interviews was not to analyze successful ransomware attacks, not all information about the incidents are known. Nevertheless, we are convinced that the reports are useful and interesting.

system. The infected device was then analyzed in an isolated network and ransomware was found. Consequently and as a precaution, they took all other legacy devices from the internet immediately[5], which was not part of their IRP but the outcome of a short risk assessment. Additionally, they reinstalled and configured the infected device to be the 'new' backup device. Since the attack did not spread through the network, no damage was done except the lost working hours. As a result of the incident, two measures were taken. First, a policy that legacy devices cannot access the internet was reintroduced. This policy was in place beforehand but was revoked one year before the incident. Second, the network was more granular segregated to make it more difficult for a possible infection to spread.

Attack 3 (medium, 2019)
One client was infected over a malicious e-mail attachment. The attachment opened a connection to a remote server, downloaded and executed malicious code, which started to encrypt data on all accessible hard drives. As a result, employees could not access files anymore and notified the IT department, which again allowed them to react quickly, following their IRP[6]. First, they disconnected the servers to avoid further damage (spreading). Second, they located the source of the attack, shut down the corresponding client, and ensured, that it was not rebooted. Third, they continued analyzing if there were any other signs for infections[7]. Lastly, they restored the backups. Due to the fast reaction, no damage was caused except for the lost working hours. Interestingly, the interviewee pointed out that he rates their cybersecurity protection as very strong. All employees are trained during the onboarding and regularly thereafter, sandboxing is in use, and the network (connections, traffic, unknown IPs) is monitored. Nevertheless, the attachment evaded sandboxing, the employee opened it, and the network alert was only seen after first calls came in. The company did not change their measures afterwards because they think that they are on a good level.

Remark: This attack happened in the afternoon shortly before end of work, while the next day was a public holiday. Fortunately, employees were still working as otherwise the impact may have been more significant.

Attack 4 (substantial, 2016)
Again, ransomware infiltrated the company by a malicious e-mail attachment. Due to a poor user account privileges management (privileges were not granted individually), the infected device had an account with high privileges which could be leveraged to access nearly all devices including the central information system. The attack was noticed when the data on the central information system could not be accessed anymore due to encryption. As no incident response strategy was developed beforehand, the reaction was based on best knowledge of the IT department. As a first reaction, they shut down all servers to prevent further spreading. To identify the source, they manually analyzed the logs for several hours until they found it. Next, the infected device was restarted but the problem persisted, i.e., the device started to encrypt data again after booting was completed. Consequently, the machine was isolated, and the systems had to be cleaned and restored from backups, which were fortunately not encrypted. But even with all productive systems restored, the company experienced further problems as the productive systems were missing the connections to test systems and did not work without them. In the end, the company needed about 18 hours until they could start to work under restrictions again, following a basic predefined-BCP[8]. But they could just reach a small fraction of the normal throughput with the missing systems because everything had to be processed manually. After 48 hours, the company could go back to normal operations. In response to the incident, the company made several changes to their cybersecurity strategy. They reduced the privileges of user accounts, introduced application whitelisting, introduced the policy that all scripts (e.g., Excel, Powershell) need to be signed, and improved their firewall

[5]The interviewee was not sure if they analyzed the other devices for possible infections or thought that ransomware did not spread over the network because no other problems were reported.

[6]The response was in accordance with the company's IRP, but the interviewee never stated explicitly that they followed it. However, we assume that they acted according to it.

[7]Unfortunately no further information was provided.

[8]The interviewee stated that the BCP was not helpful to keep the business running.

settings. Moreover, as management experienced the attack, they are more aware of cybersecurity and are more likely to grant needed funding for proposed improvements.

Existing DFC related literature

In addition to the interviews, we looked at existing literature (resources) to see which countermeasures are frequently / less frequently discussed. We use literature in the broadest terms including research articles, blog entries and other online resources. The upcoming subsection summarizes how SC related resources compares to DFC related resources in terms of absolute numbers. Next, we express our findings with respect to refined Google scholar searches. Since we consider ransomware case studies and best practices as important, they are addressed in the last subsection.

The searches were performed using google.com as well as scholar.google.com (GS). Utilized keywords are mentioned in the corresponding paragraphs. To categorize or discard a resource, Google-headlines served as a first filter. If a headline itself did not allow for a decision, the resource was analyzed further (e.g., reading the abstract or introduction).

Remark: This is not a sophisticated literature survey but a rudimentary analysis in order to support our interview findings.

Ransomware literature

This section differentiates between Google and Google scholar results:

Google findings

The starting point was a regular Google search using 'ransomware' and focusing on the top 50 listings. Unsurprisingly, most of the listed resources were of general nature from frequently visited websites such as Wikipedia, Zdnet, Norton, McAfee or Microsoft. Additionally, there were some entries on recent incidents. A good, detailed resource we came across was from NIST, providing a series of different documents on how to get started, and how to detect and respond to ransomware attacks [11].

Google scholar findings

Searching for 'ransomware' in GS revealed 25.400 results in total where we again focused on the first 50 entries. Only two articles were identified within the DFC related area of **Recovery**: [12] describes a self-healing, ransomware-aware filesystem by monitoring low-level filesystem activity. If a process violates a previously trained model, "their operations are deemed malicious and the side effects on the filesystem are transparently rolled back". The second article (patent) by [13] suggests monitoring operating systems events which will be analyzed and if considered suspicious a backup is created. In case the misgiving comes true, it can be rolled back.

The other articles can be clustered[9] as follows (each was put into *exactly one* category):

Detection (16) includes articles focusing on automatic detection of ransomware but also manual approaches using honeypots or threat hunting.

General literature (10) includes articles describing the evolution or are very general in their nature, e.g., list steps of a ransomware attack as well as general aspects of recovery and curing[10].

Analysis (9) includes articles analyzing one or more ransomware samples either automatically, manually, or dynamically. We also included ransomware classification into this category.

Preventive / defensive measures (8) includes articles of general nature (e.g., mentioning the necessity of spam filters and anti-virus software) as well as advanced literature such as monitoring the power consumption.

Crypto currencies (4) includes articles that focus on flows of currencies in order to learn about ransomware.

Education (1) represents one article titled 'awareness education as the key to ransomware prevention'.

In summary it can be said that the highest ranked (and thus also the articles frequently cited) most fall into SC. Furthermore, none of the

[9]The clustering process followed a simple procedure: if one of the 'categories' above was mentioned in the article title, it was added to the corresponding category. If no exact match was found, we looked for similar categories, e.g., crypto currency and bitcoin. As a last resort, the categorization was done based on the abstract. In case a article would match several categories, we placed it into the category we identified as best fit.

[10]These articles are so general that we decide not to place them under 'recovery'.

articles has been a case study / best practice.

Refined Google scholar searches

We explicitly searched for DFC related resources. The utilized keywords as well as absolute number of results are shown in Table 2.

Our searches were separated into three categories: Digital forensics and ransomware, DFC related literature (both discussed in this section) and case studies/best practices (subsequent section).

Table 2. DFC related search terms and their absolute counts of identified literature items on Google scholar.

Search term	#
ransomware "digital forensics" OR "digital forensic"	1710
ransomware recovery	6130
ransomware backup	5170
ransomware "incident response plan"	433
ransomware "disaster recovery plan"	249
ransomware "business continuity management"	246
ransomware "business continuity plan"	220
ransomware "incident response management"	64
ransomware "incident response strategy"	32
ransomware "business continuity strategy"	10
ransomware "disaster recovery strategy"	8
ransomware "case study"	4080
ransomware "best practices"	3790

Digital forensics and ransomware

There is significantly less ransomware resources when searched in conjunction with digital forensics: about $\sim 7\%$ of all results. Most literature items focused on forensic readiness for ransomware (i.e., "processes provide mechanisms for the pro-active collection of digital footprints" in support of possible future digital investigations [14]), cyber investigations, memory forensic analysis of ransomware, ransomware analysis or were of general nature (e.g., titled 'the rise of ransomware and emerging security challenges in the Internet of Things' by [15]).

DFC related literature

We started with terms such as 'recovery', and 'backup' which revealed large numbers of results. However, many articles were of general nature pointing out the necessity of backups and recovery without detailed guidelines. Furthermore, we found more advanced work such as PayBreak by [16] who identified the encryption keys while the ransomware is active allowing recovering files after encryption. Other articles focused on peculiarities of SSD drives to detect and recover from ransomware attacks [17], [18]. While all of them are interesting and relevant, they cannot be easily implemented by corporations or help with a fast recovery. An exception we found was written by [19] who discuss steps to be taken before, during and after an incident.

Next, we narrowed down the searches looking into niche areas under the DFC umbrella using terms such as 'business continuity', 'incident response' combined with 'plan', 'strategy' and 'management'. Note, we understand that IRP or BCP are usually general procedure and not related to ransomware. However, we argue that due to the impact of ransomware, there should be dedicated and detailed guidelines as ransomware often has higher impact than a random failure of a system or other malware. The found resources often argued that business continuity (disaster recovery) is essential but without details on what to consider and how to kick-off the process. On the other hand, the regular Google searches provided plenty of examples. However, most of them had a commercial nature originating from companies trying to sell products and services.

Ransomware case studies and best practices

For this section we were looking for detailed descriptions that haven been evaluated by others or peer reviewed. However, while searching we felt that not many publicly available case studies exist, and that the ones that do exist are mostly short and not conclusive. They were either reported by public agencies, newspapers, cybersecurity vendors or other organizations. Moreover, it is noteworthy that extensive entries in discussion boards or forums seem to be missing. Public agencies describe in their cybersecurity reports selected case study examples. But [2], for example, just uses a few lines to explain the entire incident, while [8] outlines five cases within just a few pages. The newspaper articles are mostly of general nature and do not go into detail. Reports from cybersecurity vendors seem to highlight their products and solution the most. Scientific papers which focus on case studies (e.g., [6]) use the results from their analysis for their research but do not publish extensive information about the use cases themselves. Also, we noticed that

reports which are more detailed mainly focus on measures we consider falling under SC. [20], for example, describe four cases in detail focusing on attack vector, attack steps and the aftermath of the attack.

For best practices, we found an abundance of recommendations, either from official government sources, cybersecurity vendors, in the form of scientific papers or blog entries. Most of them focus on SC and only briefly mention DFC related ransomware best practices. Moreover, the ones that target the latter, either focus on advertising or are not detailed enough to be of real help. They present the threat of ransomware, shortly talk about the recovery strategy, and then present their fee-based solution. A good starting point for a ransomware recovery guideline is [19] that lists five steps on how to create a ransomware recovery plan and later explains what to do before, during and after a ransomware incident. However, we feel it is not detailed enough to be used as step-by-step instructions.

To conclude, while several case studies and best practices have been released, they are not detailed enough that interested individuals can easily apply them (e.g., to improve their own strategies).

Discussion

This section addresses the questions raised in the introduction.

Q1: Given ransomware countermeasures recommendations, which measures are actually implemented by businesses and which are not?
Comparing our interview answers with the recommended countermeasures reveals several gaps. While there seems to be a strong focus on technical solutions such as vulnerability patching, monitoring or anti-virus, as well as network security, there is a tendency to neglect social, organizational, and procedural aspects. One reason for the popularity of technical measures may be the ease of deployment compared to other recommendations, e.g., installing a piece of software vs. developing and testing recovery strategies (or continuous training and education). Another influencing factor may be the media ads: there are more commercials for products than for processes such as an Incident Response Plan (IRP) or Business Continuation Plan (BCP). When asking the interviewees about the most important measures, two argued for training, four saw a mixed approach of training and technical measures as most efficient, and two named technical measures.

An interesting observation was that while the user is often classified as the 'weakest link', they detected in three of four successful ransomware attacks the infection better (faster) than other mechanisms in place. In other words, users identified that the systems were infected, immediately reported and consequently limited the damage caused by ransomware. However, we found that user education and training are often only done once (e.g., during on-boarding), or use inadequate modality, for example e-mail newsletters or online training, instead of recommended face-to-face training.

Lower attention is given to recovery, especially recovery procedures. While backups are frequently mentioned and widely common, measures such as IRP, BCP or communication plan, are lacking; hence there is only an incomplete recovery strategy. A reason for the under-utilization of these recovery measures could be that they are perceived as inefficient. Multiple interviewees stated that BCP is not helpful because it can never be as efficient as the regular process, which was also shown during one of the presented attacks.

Q2: How do available online resources compare to given ransomware countermeasure recommendations?
During our analysis we found that there is a significant imbalance between online resources and countermeasure recommendations: Online resources primarily focus on creating techniques for prevention, detection, and prediction (mainly technical measures), while guidelines [2], [3], [4] also stress the importance of other areas such as an advanced recovery strategy. A possible reason for why there is not much DFC resources on non-technical aspects of ransomware is that private companies want recovery over a thorough investigation[11]. Another reason may be that management/administrators still believe they are able to prevent infections and hence focus all money and efforts towards prevention and prediction. However, we believe it is important to share

[11] This argument was raised by a reviewer.

findings, e.g., was a backup strategy successful, what worked well (and what did not), how long did the actual recovery require and what are the lessons learned.

Q3: How can the digital forensics community help to combat ransomware?

We believe there are two major aspects:

Foster collaboration and exchange: Sharing detailed resources for all recommended ransomware countermeasures is essential which is not the case. For instance, some interviewees stated that they only provided insights as they are curious to see how the situation is in other companies, i.e., which measures they implement, if they have been attacked, and if yes, how they reacted. One may argue that exchange platforms already exist like CERTs (Computer Emergency Response Team) or the "Global Cyber Security Center, with its OF2CEN[12] advanced information exchange platform [... which fosters] a strong collaboration with Italian and International government institutions, private bodies, research institutions and international bodies" [21]. However, none of the interviewees mentioned any company consortium which means they are either unaware or there are other constrains why they are not participating. If participants are worried about their reputation, anonymous platforms could be created.

Improve quantity, accessibility, and comprehensibility: While a lot of resources in all areas have been published, they are insufficient as ransomware attacks still occur and recovery often does not work appropriately. Maybe existing guidelines and recommendations are too theoretical or too complex to understand and implement. Other reasons could be the missing expertise in the company, not seeing the value of countermeasures or confusion of these concepts. We argue that sharing best practices[13] in all detail would provide an additional resource which may help companies to understand the importance of all countermeasures and recover faster.

[12]The related EU Project is called EUOF2CEN (https://www.commissariatodips.it/euof2cen.html).

[13]Note: we focus on best practices / case studies and not policies as provided by ISO or NIST.

Conclusion

For this article, we analyzed existing ransomware countermeasure recommendations and then conducted a qualitative survey (interviews) to understand which countermeasures have been implemented by companies. The results show that companies primarily focus on technical security measures and network security, but neglect user security education, security policies, awareness of management, and incident response strategy (including incident response plan (IRP), business continuity plan (BCP), and communication plan). Secondly, we searched for existing ransomware literature and compared its quantity with the recommend countermeasures (taxonomy). We found that research is primarily conducted on technical measures and network security (which is identical to the most frequently implemented countermeasures by companies). On the other hand, we found that literature under the DFC umbrella often lacks details. More explicitly, we looked at ransomware surveys and case studies, and concluded that they are often general, which makes them less relevant/helpful. To improve the situation, the DFC should collaborate more and should work on and provide more detailed resources (best practices).

REFERENCES

1. L. Ingham, "Garmin admits ransomware attack, but has its reputation been harmed?" *Verdict*, vol. Online, July 2020. [Online]. Available: https://www.verdict.co.uk/garmin-back-ransomware/
2. MELANI, "Lage in der Schweiz und International: Halbjahresbericht 2019/1 (Januar - Juni)," Melde- und Analysestelle Informationssicherung, Tech. Rep., October 2019. [Online]. Available: https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2019-1.html
3. BSI, "Die Lage der IT-Sicherheit in Deutschland 2019," Bundesamt für Sicherheit in der Informationstechnik, Tech. Rep., October 2019. [Online]. Available: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/bsi-lagebericht-2019.pdf?__blob=publicationFile&v=4
4. US-CERT, "Ransomware: what it is and what to do about it? technical guidance document 2017," Department of Homeland Security, Tech. Rep., 2017. [Online]. Available: https://us-cert.cisa.gov/sites/default

/files/publications/Ransomware_Executive_One-Pager_and_Technical_Document-FINAL.pdf
5. Jan Huck, “Ransomware countermeasures in the extended Rhine valley A comparative analysis of companies’ implemented ransomware strategies,” Master’s thesis, University of Liechtenstein, 08 2020.
6. L. Y. Connolly and D. S. Wall, “The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures,” *Computers & Security*, vol. 87, p. 101568, 2019.
7. S. Kraemer, P. Carayon, and J. Clem, “Human and organizational factors in computer and information security: Pathways to vulnerabilities,” *Computers & security*, vol. 28, no. 7, pp. 509–520, 2009.
8. BSI, “Ransomware: Bedrohungslage, Prävention & Reaktion 2019,” Bundesamt für Sicherheit in der Informationstechnik, Tech. Rep., December 2019. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.pdf?__blob=publicationFile&v=6
9. MELANI, “Vorsicht: Weiterhin erhöhtes sicherheitsrisiko durch ransomware gegen kmus,” Melde- und Analysestelle Informationssicherung, Tech. Rep., February 2020. [Online]. Available: https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/sicherheitsrisiko-durch-ransomware.html
10. A. Fagioli, “Zero-day recovery: the key to mitigating the ransomware threat,” *Computer Fraud & Security*, vol. 2019, no. 1, pp. 6–9, 2019.
11. NIST, “Ransomware protection and response,” National Institute of Standards and Technology, Tech. Rep., 2021. [Online]. Available: https://csrc.nist.gov/projects/ransomware-protection-and-response
12. A. Continella, A. Guagnelli, G. Zingaro, G. De Pasquale, A. Barenghi, S. Zanero, and F. Maggi, “Shieldfs: a self-healing, ransomware-aware filesystem,” in *Proceedings of the 32nd Annual Conference on Computer Security Applications*, 2016, pp. 336–347.
13. H. Ye, W. Dai, and X. Huang, “File backup to combat ransomware,” Apr. 19 2016, uS Patent 9,317,686.
14. A. Singh, A. R. Ikuesan, and H. S. Venter, “Digital forensic readiness framework for ransomware investigation,” in *Digital Forensics and Cyber Crime*, F. Breitinger and I. Baggili, Eds. Cham: Springer International Publishing, 2019, pp. 91–105.
15. I. Yaqoob, E. Ahmed, M. H. ur Rehman, A. I. A. Ahmed, M. A. Al-garadi, M. Imran, and M. Guizani, “The rise of ransomware and emerging security challenges in the internet of things,” *Computer Networks*, vol. 129, pp. 444–458, 2017.
16. E. Kolodenker, W. Koch, G. Stringhini, and M. Egele, “Paybreak: Defense against cryptographic ransomware,” in *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, 2017, pp. 599–611.
17. D. Min, D. Park, J. Ahn, R. Walker, J. Lee, S. Park, and Y. Kim, “Amoeba: an autonomous backup and recovery ssd for ransomware attack defense,” *IEEE Computer Architecture Letters*, vol. 17, no. 2, pp. 245–248, 2018.
18. S. Baek, Y. Jung, A. Mohaisen, S. Lee, and D. Nyang, “Ssd-assisted ransomware detection and data recovery techniques,” *IEEE Transactions on Computers*, pp. 1–1, 2020.
19. B. Kenyon and J. McCafferty, “Ransomware recovery,” *Itnow*, vol. 58, no. 4, pp. 32–33, 2016.
20. Alliance for Healthier Communities, “Cybersecurity and ransomware: Alliance member case studies,” Alliance for Healthier Communities, Tech. Rep., 2019. [Online]. Available: https://www.allianceon.org/sites/default/files/documents/A%20casestudy%20of%20Ransomware%20Attacks-EN_0.pdf
21. European Cyber Security Organisation (ECSO), https://ecs-org.eu/documents/publications/5c0a6a3aac673.pdf.

Jan Huck is an information security professional in a Swiss cybersecurity company. He advises and accompanies different clients operating in various industries. Jan elaborates and evaluates security strategies, concepts and risk minimizing measures; develops and implements information security management systems (ISMS); and acts as external CISO.

Dr. Frank Breitinger is an Associate Professor at the University of Lausanne (Switzerland). Prior, he was an Assistant Professor at the University of New Haven (US) where he acted as the co-director of the Cyber Forensics Research and Education Group and at the University of Liechtenstein at the Hilti Chair for Data and Application Security. His teaching and research interests are cybersecurity and digital forensics. Additional information about him and his work is on his personal website (https://www.fbreitinger.de).