AMSTERDAM ENTREPRENEURSHIP CASES:

Author:
Joris Ebbers
Associate professor Entrepreneurship and Innovation
University of Amsterdam
March 20, 2019

Introduction

"We see ourselves as hacking a new business model for prototyping an ideal company that optimizes for benefits to the world (customers, employees, society) rather than financial interests (shareholders, investors, founders).
[Melanie Rieback, CEO and founder of Radically Open Security]

Radically Open Security (ROS) is an IT security platform founded by Melanie Rieback in 2014 and based in Amsterdam, the Netherlands. ROS is a nonprofit business, whose organizational structure is based on "ethics by design": prohibiting dividends, investors, and exits, and using business as a vehicle for positive impact.

The majority of the work ROS does, consists of so-called "pentesting". Pentesting is short for penetration testing, which is an authorized cyberattack to evaluate the security of IT systems by trying to exploit its vulnerabilities. This includes websites, mobile apps, infrastructure, cryptography, and embedded systems, which is an integration between physical objects and computing including (but not limited to) Internet of Things. In addition, they perform lock picking and social engineering tests that are about exploiting the human factor, such as phishing and mystery guest attacks. Finally, they are hired for incident response where they help customers with particular incidents such as data breaches.

In 2018 ROS had about 80 customers and €750.000 turnover. ROS serves the following sectors: government, police, financial, insurance, Internet, energy, water, retail, media, software, universities, SMEs, startups, NGOs, and nonprofits. Customers include retailer

Ahold Delhaize, insurance company Aegon, internet organizations Mozilla and Google, and TenneT, the national electricity transmission system operator of the Netherlands.

> *"Uber is a taxi company that doesn't own a single car. Airbnb is a hotel company that doesn't own a single piece of property. We are a pentesting company that doesn't have a single pentester."* [Melanie Rieback]

Being a platform business, ROS is a 100% virtual organization that does not have a physical office but manages a network of freelance pentesters, most of whom are also active in the global hacker and open source community. Currently, this network consists of around 40 freelancers, which translates to roughly 15 FTE. At least 70% of these freelancers live and operate from outside ROS's home base, the Netherlands. They hire freelancers from all over the world including Germany, Australia and India, and countries in the Middle East and Latin America. They hardly meet face-to-face and mainly use ROS's online tools such as RocketChat for communication and Gitlab for storing and processing pentest reports.

Box 1: Profile of a ROS pentester

Stefan Grönke started programming at the age of 10. When he was sixteen he started a company with a friend to build websites, and from simple websites it went to web applications and beyond. He does not have a formal IT or security education but learned everything himself. At some point, he started to work as a software developer for larger companies. However, this was a frustrating experience because he always had a strong eye for security. Instead of treating security as an afterthought once a software product is almost ready, he strongly believes in security by design where security is the starting point.

> *"I was going to stand up meetings in the morning and complain about security issues. I mentioned in the meetings 'hey guys: this is important, we need to fix this first, we need to address some architecture and design problem in this application'. But mostly nobody appreciated that. It felt more like I'm annoying to them."*

Two years ago, after attending a security conference, he shared this frustration with a friend who already worked as a pentester for ROS. His friend told him about ROS, suggested to contact them, and introduced him to Rieback. When there seemed to be a match, ROS gave him the opportunity to work on his first pentest for ROS together with this friend, who also onboarded him and made him familiar with all of ROS' tools and work processes. This first project was entirely remotely. In the beginning, Grönke mostly preferred to work from his home town Trier, Germany, which is close to the border with Luxemburg. Since some customers want pentesters to work onsite, he started to work more at the customer's office, especially in the Amsterdam region, which is not too far from Trier. Nowadays, he actually enjoys these onsite projects very much, and works around 50-50 offsite and onsite.

ROS is a perfect fit for him because he likes the flexibility of the projects. However, he would not recommend ROS to people who are looking for a regular full-time employment job, like to go to a physical office, and need structure. *"There is no office you can go to, so you have to take care about yourself and that's not the best for everybody [Stefan Grönke]."* Currently, his life is split in two. On the one hand, some occasional consulting jobs aside, he is a self-employed freelance pentester for ROS. On the other hand, he is an open source developer of defensive software that people can use to protect themselves against frauds and dangers that come from the Internet, computers and other use of technology.

Grönke meets many people that he likes to work with through his open source projects. In addition, he meets them at cyber security conferences such as the *Chaos Communication Congress* he recently gave a talk about how people can defend themselves against fraud. Besides hooking up with people who already work for ROS, to go for lunch or grab a beer together, this kind of conferences are also a good place to build up new contacts. Some of these people he met during these conferences, he also introduced and recommended to ROS. However, before doing so, he first made absolutely sure that these people share the same values as ROS, particularly when it comes to ethics, transparency, and open source.

How it started

CEO Rieback has a BSc in biology and computer science from the University of Miami, a MSc in computer science from Delft University, and a PhD in computer science from the Vrije Universiteit Amsterdam (VU). Her PhD dissertation was concerned with security issues related to radio frequency identification (RFID) technology. RFID technology uses electromagnetic fields to identify and track tags that can be attached to objects such as cars, clothing, animals, public transport cards, and is sometimes regarded as a replacement for barcode technology. After completing her PhD dissertation, she stayed at the VU as an assistant professor in computer science, while also creating a hardware solution called *RFID Guardian.*

After being unsuccessful in getting the *RFID Guardian* into manufacturing, and realizing that she did not want to pursue an academic career, she decided to move to Vancouver, Canada, to work for software company *Citrix* where she wound up being the Senior Engineering Manager and manager of the local office. After this office was shut down practically overnight because the product performed below expectations, she decided to move back to the Netherlands where she found a job at the Cybercrime Emergency Response Team (CERT) of ING Bank. Little over a year later, because of some negative experiences she had on the job, she was inspired by the idea of starting Radically Open Security, and within a week after having the idea she handed in her resignation letter at ING Bank.

Rieback rounded up a team of 6 other people from her network to start ROS: John Sinteur, who had over 20 years of industry experience in IT infrastructure and architecture, and worked for Dutch telecom company *KPN* and startup *FarMedvisie;* Jan-Mark Wams, former colleague at the Vrije Universiteit Amsterdam, serial entrepreneur, and founder of *Coders Co.*; Sake Blok, co-developer of *Wireshark* with expertise in network monitoring; Jurriaan Bremer and Claudio Guarnieri, both involved in *Cuckoo Sandbox,* an open source automated malware

analysis system; and Peter Geissler, who according to Rieback is a "*super amazing hacker*". Besides helping get ROS of the ground, these people also helped to attract a lot of media coverage for their high-profile hacking projects. About two years after ROS was set up, most of these people moved on. Rieback is still on good terms with all of them.

Out of this original group of 7 people, 2 are still active at ROS: Rieback and Sinteur. While Rieback is the CEO and external face of the company representing ROS at customers and events, Sinteur is in the lead in developing ROS' online infrastructure and programming tools. Wams played a significant role in ROS' nascent phase by offering Rieback to invest €500.000. After Rieback used Wam's €500.000 investment pledge to round up a number of highly talented pentesters and attract some launching customers, eventually she turned down Wam's investment offer and instead bootstrapped ROS out of her own personal savings. However, in the early phase, Wams did provide Rieback with valuable business advice, especially about ROS' legal structure and financial management, and provided a couple of small short-term cash flow loans.

Finally, an important role was played by the NLnet foundation. NLnet pioneered the world's first internet dial-in and ISDN infrastructure with full country coverage in the Netherlands. In 1997, its commercial activities were sold to UUnet – now part of US telecommunications company Verizon – and since then, NLnet has focused on supporting organizations and individuals that contribute to the open internet, and the privacy and security of internet users. NLnet funded Rieback's PhD research at the VU where they had close contacts with the Computer Science department, including Rieback's PhD supervisor Prof. dr. Andrew Tanenbaum. Besides offering practical support, including ROS business cards and laptop stickers, a year after Rieback started ROS, NLnet provided 2 small loans to help Rieback deal with cash flow swings caused by the fact that their large customers have a 60-day payment term, while ROS pays their pentesters within 30 days.

Hacking a new nonprofit business model

> *Our hope is that we inspire others to set up similar sustainable nonprofit businesses in other industries. Call us dreamers, but we hope that we can help to move society forward in this way." (Melanie Rieback]*

Inspired by a new wave of economists, who argue that our addiction to growth (GDP) is unsustainable, causing climate change, human rights violations, threats to biodiversity, and unprecedented waste, Rieback sees ROS as a prototype of so-called "post-growth entrepreneurship" for those aspiring to flat growth curves and creating non-extractive businesses. In addition, while the social business, as envisioned by Nobel Prize winner Muhammad Yunus, was defined as "no-dividend business for solving human problems", the no-dividend idea got lost. Instead, Rieback propagates "ethics by design": prohibiting dividends, investors, and exits, and using business as a vehicle for positive impact.

With that philosophy in mind, Rieback chose the legal structure of a Fiscal Fundraising Institution (FFI)[1] for ROS. The idea for adopting this usual legal structure was raised by Michiel

[1] Fiscaal Fondswervende Instelling in Dutch

Leenaars, who was (and still is) director of strategy at the NLnet foundation. After Rieback finished her PhD at the VU she always stayed in touch with NLnet in general, and Leenaars specifically. At some point, when brainstorming about the particular legal structure Rieback had in mind for ROS, she told Leenaars that she did not aspire to building a traditional for profit company. However, she also did not want to be restricted in running a financially sustainable business.

According to Rieback, the FFI appeared to be an interesting *"business model hack"* because it forces organizations to be social because they need to give away their profits to a charitable foundation with a so-called ANBI status.[2] It is a construction that started off with churches in the Netherlands engaging in commercial spin-offs that wanted to channel their profits back into the church while enjoying tax benefits. A famous example of an FFI is the Language Institute Regina Coeli, also popularly known as the *Nonnen van Vught* (Nuns of Vught]. However, to avoid accusations of tax evasion that have been associated with the FFI structure, ROS also pays corporate income tax like any normal business[3].

Being an FFI, ROS is legally obligated to give their profits – in the sense of dividends – to a foundation of their own choice. Since ROS chose the NLnet foundation as their beneficiary, they are contractually committed to giving away their profits to NLnet. Besides having to give away its profits, being an FFI, ROS needs to meet two other requirements. First, because the tax authorities want to make sure that organizations using the FFI status are indeed charitable, they need to have a minimum number of volunteers. Second, ROS is only allowed to keep one year's worth of turnover in cash at any given time. If they have more, they are legally required to give it to NLnet. However, currently a large amount of revenue is being reinvested in growing ROS. Notwithstanding, they have made two donations to NLnet.

In term of ROS' governance structure: At the top of ROS is a foundation. The board of this foundation[4] has three members: the two co-founders Rieback and Sinteur, and Prof. Tanenbaum of the VU. The sole purpose of this foundation is to own the shares of the Limited Company / FFI [5] and to select a new director in case something happens to Rieback. Nothing can be done without a unanimous decision by all three members of the board. In addition, ROS has an advisory board consisting of three members: Prof. Tanenbaum, who is also in the board of the foundation, NLnet, and Ian Cook. Cook is a well-known security research and intelligence analyst. These board members provide informal advice, share their views, and occasionally refer new colleagues or customers.

Radical about openness and security

One of the main motivational drivers of Rieback for starting with Radically Open Security, was that established IT security companies are not very open or transparent with respect to their customers about the way they operate. The business model of these established companies could be described as a black box approach, where pentesters search for security weaknesses without involving the customer in the process. In other words, instead of helping the

[2] ANBI stands for Algemeen Nut Beogende Instelling
[3] Vennootschapsbelasting in Dutch.
[4] Stichtingsbestuur
[5] Besloten Vennootschap (B.V.)

customer to learn from the experience themselves, they keep their customers in the dark so they can more easily sell repeat business.

> *"Our core principles of "no sketchy stuff", "teach to fish" and "open-source" are a popular selling point that most of our competitors cannot match because such altruistic aims run counter to their business model"* [Melanie Rieback]

In contrast, ROS is very transparent towards its customers and the wider IT security community. First, they developed a "ChatOps" infrastructure that uses chatrooms and chatbots to allow customers to "Peek-Over-Our-Shoulder" and observe each and every step their pentesters take. In other words, ROS actively facilitates knowledge transfer to their customers by providing a "free training" with every pentest. Second, ROS shares all the IT tools that they developed by making them freely available as open source. This is nicely illustrated by one of their pentesters, Stefan Grönke (see also Box 1):

> *"So, you're speaking out loud in the channel so that the customer can also see what you're doing. That's also the way you communicate with your colleagues [other pentesters]. You discuss ideas, what to do next, and come up with a plan."*

At the moment, ROS' online platform has more than 100 channels. However, not everyone automatically gets access to all of these different channels. Figure 1, for example, shows the screenshot of a simplified online environment for a fictitious pentester called "H.Acker". This person has access to 7 chat channels ("Conversations") that are listed in the black box on the left-hand side of the screenshot:

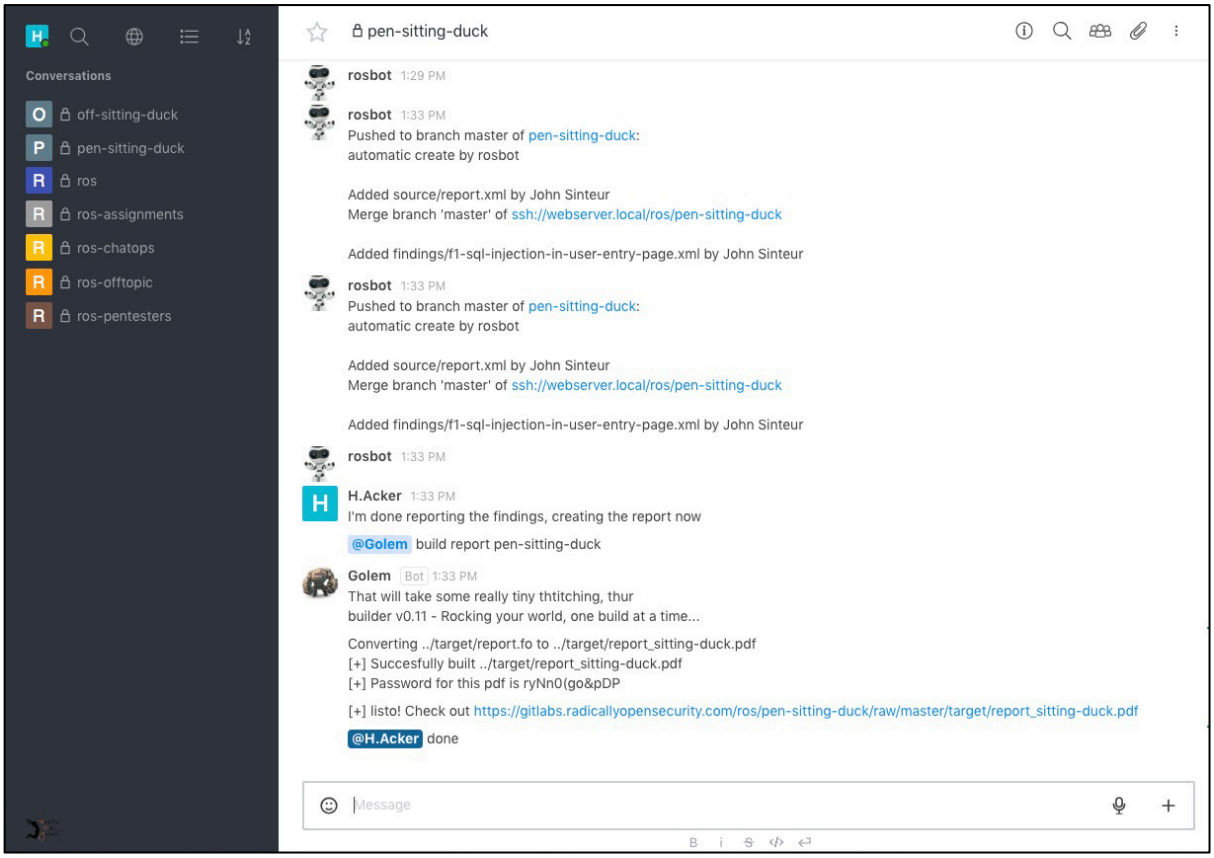
1. "off-sitting-duck": The channel where the quote is discussed with the customer, including setting the scope and time planning[6].
2. "pen-sitting-duck": The channel where the pentest is being executed together with the particular customer ("Peek-Over-Our-Shoulder").
3. "ros": The generic channel for all Radically Open Security people for subjects that don't fit in any of the other channels.
4. "ros-assignments": The channel for all Radically Open Security people where all the incoming jobs are handed out on a first-come-first-serve basis.
5. "ros-chatops": The channel for all Radically Open Security people where the functioning of chat itself is discussed.
6. "ros-offtopic": The channel for all Radically Open Security people for things that are not directly related to Radically Open Security or its customer.
7. "ros-pentesters": The channel for all Radically Open Security pentesters to ask for advice and discuss generic things about executing pentests.

Channels 1 and 2 are accessible to customers. Channels 3-7 are for ROS people only. Channel 6 (the off-topic channel) is used by pentesters to post links that can be interesting for the ROS community, including early warnings about IT security issues, such as the recent Meltdown and Spectre vulnerabilities on chips and processors used for personal computers, mobile devices and the cloud (see figure 2). Channel 7 is the place where pentesters can turn for help

[6] "off" comes from the Dutch word for quote: offerte

and advice, for example by asking for particular software or hardware. In figure 1, one important channel that is part of the heart and soul of ROS – "ros-ethics" – is missing. This is where ROS discusses ethical questions, including whether or not to accept certain customers.

Figure 1: Simplified example ROS' online environment

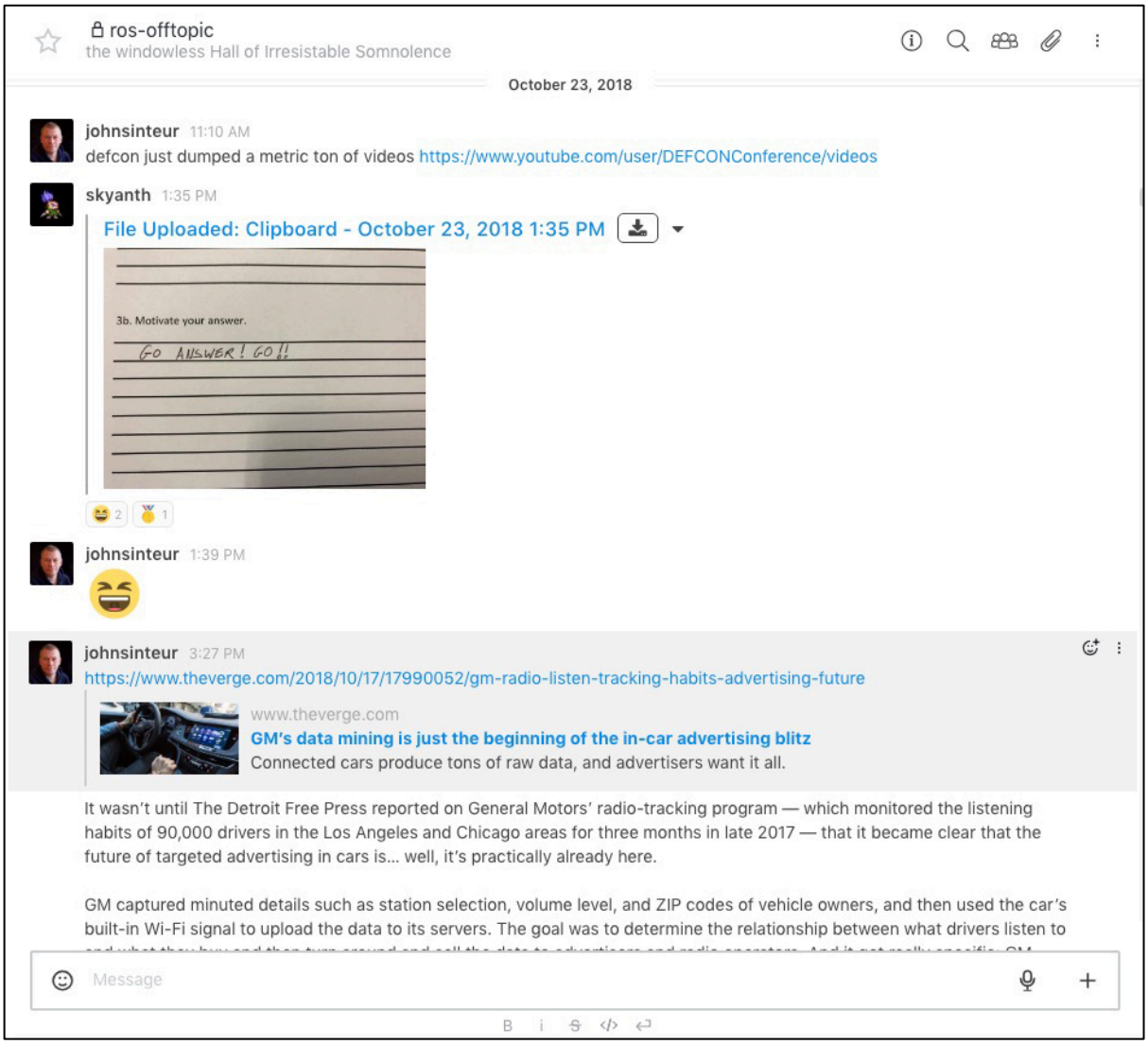


Convincing the customers

> *"At the beginning when I told people I wanted to create a nonprofit security consultancy company, people were like: 'What? It's never going to work. Big companies are never going to trust you. Why would they trust you? They're not going to understand what your intentions are.'"* [Melanie Rieback]

In ROS' early startup phase, an important role was played by a small number of "*early adopter geeks*" that Rieback knew from the hacker community. The fact that ROS is a nonprofit business that adheres to the values of the open source community helped to attract new customers through former ethical hackers who got jobs as IT security specialists at a wide variety of organizations, including large corporations. Besides having the technical background to understand that ROS has exceptional expertise in their network of highly talented freelance pentesters, these IT security specialists also played an important role in convincing their skeptic colleagues.

Figure 2: ros-offtopic



An example of these people is Florence Mottay, VP Information Security and CISO Europe at Ahold-Delhaize, one of ROS' largest customers. Ahold-Delhaize is a large international retailer based in the Netherlands, known for supermarket Albert Heijn, liquor store Gall & Gall, pharmacy ETOS, and web shop Bol.com and with 60 % of the revenue in the US with brands like Food Lion and Stop and Shop. Mottay has a background in mathematics and computer science, and started as an ethical hacker in 2000 being a frequent visitor of information security conferences such as Black Hat and hacker conventions such as DEF CON. Today, she still has one foot in the hacker scene to keep up to date and catch up with friends. When entering the corporate world, IT security experts such as Mottay, faced some cultural differences. Mottay:

> *"When I started in this field almost 20 years ago, no one in this industry was corporate material – we were a bit of a quirky group. Our job was to find exploits and look for vulnerabilities before systems went into production. And that was it.*

Mottay was introduced to Rieback by Benessa Defend, a colleague of Mottay's at Ahold-Delhaize, at a security event in the Hague, the Netherlands. At the time, Mottay was not impressed with the quality of the pentests that they were getting. She therefore organised a beauty contest for which she also invited ROS. A beauty contest, in this case, meant that every contestant had to test the same application to demonstrate their skills, and needed to deliver a test report free of charge. After Mottay picked ROS as a supplier because of their exceptional skills, she had to convince some of her colleagues who felt somewhat uneasy about working with a nonprofit business that consists of a loose collection of idealistic freelance hackers. For example, she had to explain to them that one needs to distinguish between "*white hats, and black hats, and people rarely cross",* where the former are ethical hackers:

> *"After meeting ROS, they [Mottay's colleagues] had some concerns and mentioned 'they're hackers, they're not even full-time employees, we have no control, and it's a nonprofit.' And when they met Melanie, they said 'she's not your typical business person'."* [Florence Mottay]

Especially the legal department was concerned that they would expose their company's IT systems to people who are not employees, but contractors of ROS. They were not sure that they would not have a grip on them. By asking her colleagues to trust her, Mottay put her own reputation on the line. Although there is the option of performing a background check to screen pentesters, Mottay views this as a "*small layer of defence"* because even malicious people can pass such a background check. Instead, the reputation mechanism is a lot more effective because in IT security *"there's at most two degrees of separation, so you always know 20 people in common. If you don't, there's something wrong*".

In case a customer insists on a pre-employment screening of ROS pentesters, Rieback will ask these freelancers if they voluntarily want to do this. If they say no, that's their prerogative. But it does mean that they will not be able to work for that particular customer. Usually customers, such as banks or insurance companies, have their own commercial partner that does the screening for them. Some customers just want an official statement from the government that the person in question has not (recently) committed any criminal acts that are related to their current job.[7] However, when recruiting new pentesters ROS also prefers reputations over screenings. Rieback:

> *"What I have more faith in is social currency in the actual community, because people know when other people are screwing around…if they don't think the friend is good, then they're not going to refer them. And I actually have far more faith in that, as a check and balance, as a control, than in the screening."*

Organizational design and management philosophy

Since ROS does not have a physical office, Rieback has most of her business meetings in public cafés. The interviews with Rieback that were conducted for this teaching case, for example, took place in a café called Dok 48 in Amsterdam's recently reclaimed island IJburg. However,

[7] This is called a *Verklaring Omtrent Gedrag* in the Netherlands

ROS does have a "fake office" in the city center of Amsterdam, roughly located between the Rijksmuseum and music venue – and former church – Paradiso, made available by her friend Jan-Mark Wams at the headquarters of his company Coders Co., which she mentions on ROS' website. In the early days of ROS, customers insisted on meeting in ROS' office, but Rieback has not used this office in years. Rieback:

> *"I speak openly about our fake office, quite lovingly. It's in case a customer insists that we meet in our office, then our name is basically hanging in the window…It looks nice on the website. But the truth of the matter is, I have a 100% virtual organization, so actually having an office is completely meaningless and pointless."*

While a fraction of ROS' projects require pentesters to be physically present at the customer's office, mostly in the Amsterdam region, the majority of pentests are performed from remote locations. Rieback is therefore a strong believer in decentralized management systems and has the goal of decentralizing as much of ROS' processes as possible. To that end, ROS designed detailed work flow processes, standard documentation templates, automated tools for performing pentests, and controlled access rights on its online environment.

> *"I don't believe in top-down hierarchy, and I especially don't believe in top-down hierarchy when working with hackers. They're not so big on hierarchy. And if you basically say; 'do this'. Why?' 'Because I said so', that logic doesn't work with them. And the other thing is, if you hire people that are sufficiently good, they're actually going to know better than you what to do. So, the thing is, you just basically need to let them figure out what they need to do, and then get out of their way."*

In designing her organization, Rieback was mostly inspired by Frederic Laloux's book *Reinventing organizations*. In addition, she picked up some ideas from Brian Robertson's book *Holacracy*: *The new management system for a rapidly changing world*. Both authors advocate a decentralized management structure. However, ROS did not strictly adopt any particular management philosophy. According to Sinteur, Holacracy, for example, was designed for a context where people work together in a physical office where much of the communication takes place face-to-face instead of through online chat channels. In addition, most of ROS' freelance pentesters prefer not to be involved too much in so-called "governance meetings" to discuss (new) roles, teams and accountabilities.

ROS has defined the following core self-organizing teams and responsibilities:

1. *Project management*: managing projects, allocating projects, managing the workflow, prioritizing work, managing calendars and mailboxes, and scheduling.
2. *Business*: administering invoices, paying invoices, bookkeeping, insurance, pensions, legal, contracts, and taxes.
3. *IT and Infrastructure*: developing the platform, running operations, system administration, workflow software development (including pentesting tools).
4. *Business development*: attracting new business and customers by visiting events, giving talks, and maintaining media contacts.
5. *Pentesters:* discussing pentesting issues, asking questions and advice, sharing experiences, and discussing how to improve the pentesting process.

6. *(several short term) Engagement teams*: facilitating temporary "tiger teams" to perform a specific project, such as a pentest, which involves scoping, pentesting, project management, reviewing, and editing.

Rieback is currently mostly active in the *Project management* and occasionally the *Business development*, *IT and infrastructure*, and *Pentesters teams*. She is not involved in the *Engagement teams*, where the actual projects for customers take place, to avoid micro managing. Rieback's business partner Sinteur is predominantly active in the *IT and infrastructure, Project management*, *Business development* and occasionally specific *Engagement* teams. Steven Djohan and Anh Tran, who both also work for technology consultancy company *Revnext*, are the most active members of the *Project management* team and support Rieback on a daily basis:

> *"Nowadays the way that it works is that every morning the head of my project management team says in a chat room: 'this is the list of things that are going on and. these are the To Do points for today. Melanie, I'm highlighting you for these particular things that we need you for, so only pay attention to these'."*

Being a virtual organization with freelance contractors of which about 70% lives abroad, ROS does not have many social events. Instead, identification and long-term relations are built on ROS's online platform, where particularly the "ros-offtopic" chat channel helps in creating a sense of identification and shared culture. Occasionally, when ROS affiliates from abroad visit the Netherlands, ROS organizes a social event. For example, they participated in an escape room challenge in Amsterdam, where one of the ROS people with lock-picking skills managed to open a suitcase that contained crucial information for the challenge. In addition, most ROS people meet at conferences or hackathons such as *Chaos Computer Club* events.

What's next?

An interesting question is how the traditional companies offering IT security services will react to ROS' rise to prominence, whose philosophy and work practices seem to resonate strongly with both customers and freelance IT security professionals, and particularly self-employed pentesters. These incumbents might have started to fear losing their talented people to ROS, and looking for ways to make themselves a more attractive place to work. However, Rieback is not concerned about any potential competitive reactions by incumbents that could hurt ROS' because she believes the underlying for-profit business model of these traditional companies is highly unlikely to change. According to Rieback:

> *"They [incumbent IT security services companies] understand that it's about helping them [customers] and educating them, rather than turning profit, and that makes us more attractive. This is why the bigger companies are starting to panic. We are stealing their staff. We are stealing their customers. It's totally David and Goliath. They're completely correct to be nervous."*

At the moment, ROS has two focus areas for the near future: improving the work flow, and recruiting talent. First, ROS is continuously developing its IT infrastructure, tooling and work processes. With most of its pentest related tooling in place, ROS is now focusing on

configuration management using “containerization” software, such as Docker, which turns IT infrastructure into code that enables you to build a template. Next, you can use this template to create separate – containerized – virtual machines for each specific project. The reason for doing this this are threefold: (1) it further limits the risk of data breaches, (2) it makes it easier to transfer all the data and information from the ROS to the customer environment when a particular project is finished, and (3), it meets the very strict security requirements of some customers, for example payment providers, that want to avoid any external connections to the Internet and instead want Gitlab and RocketChat to run on their own IT infrastructure.

Building this IT infrastructure is challenging because, contrary to the hours of freelance pentesters that are directly billable to the customer, the hours spend on building ROS’ IT infrastructure are non-billable overhead costs. In addition, building IT infrastructure is expensive. A freelance developer, for example costs around €75-100 per hour. If ROS were to hire a fulltime employee, it would cost them around €75.000-100.000 per year, which amounts to about 15% of annual turnover. At the moment, ROS can afford to hire an IT infrastructure developer for about 5 hours per week. A possible solution would be to make (some of) these hours billable, by offering these IT infrastructure services to customers.

Second, recruiting freelance pentesters is a challenge throughout the IT security industry because pentesters, and especially the good ones, are rare. However, ROS has a competitive advantage over other IT security companies because their pentests can be (and in most cases are) conducted online and offsite. As a result, pentesters who work for ROS can be based practically all over the world, and do not need to relocate in order to be close to a specific physical office. In addition, ROS’ values and mission resonate strongly with pentesters that are often also active in the open source and ethical hacker communities. This makes it relatively easy for ROS to attract talented pentester through referrals by people that already work for ROS, and who are often also active in these two – often interlinked – communities.

> *“One of my main aims is stability, quality assurance, and providing the best experience for customers as well as staff members. This is because it’s a two-sided platform and we need both the producers and the consumers, and both the producers and the consumers need to be happy.” [Melanie Rieback].*

New recruits are brought in for a real pentest for a customer, which they perform together with a senior pentester who also familiarizes them with ROS’ work flow. In case it turns out that the newcomer does not have the required skills, the customer will not notice because the senior pentester will take over and finish the job. Once recruited, quality control of pentesters is mostly based on informal evaluations by fellow ROS pentesters because roughly 90% of the projects are performed in (small) interdisciplinary teams. When individuals (consistently) underperform, Rieback will hear about this. Finally, like any other platform business, over hiring is a problem because pentesters need to have enough work or they will become unhappy and leave. On the other hand, if there are too many customers this is a problem because ROS cannot deliver their services (fast enough).

Finally, with ROS firmly on track, Rieback has found more time to refine and promote ROS’ nonprofit business model to shake up other markets. Although she considers the FFI structure she chose for ROS as an interesting prototype, one of its limitations is that it cannot be used

outside the Netherlands. She is therefore exploring other legal structures with a legal expert. Through her new organization *Nonprofit Ventures,* she now helps other entrepreneurs who also want to set up a nonprofit business by providing a template for a legal document and a business incubation program based on the principle of "ethics by design", which prohibits dividends, investors, and exits. Finally, she is also pilot testing an extra-curricular Master level module on post growth entrepreneurship at the VU. Through all of these activities, Rieback hopes to fulfil her mission of shaking up any kind of market that is currently dominated by traditional for-profit companies.