rpi

HACKED

In cyber security, the same is true, and many organisations learn their weaknesses by falling victim to threats.

Cyber criminals are an innovative species, which means that as time goes on, more areas of your digital infrastructure can become security weaknesses, and once-impenetrable barriers can become trivial to breach.

That means the burden of anticipation is enormous. Your cyber security leaders need to protect against methods of attack that have happened before, are happening now, and might happen in the future.

Here are three cyber security lessons that organisations learned the hard way...

A cyber attack takes place every

39

seconds.

varonis.com/blog/cybersecurity-statistics

Lesson 1: Imitation is the sincerest from of security breach.

In 2020, a major US software provider was hacked, and through that business, cyber criminals were able to access the systems and data of over 30,000 customers, among which were state and federal agencies.

First, they breached the software provider's security and injected a malicious code into the piece of software that the provider sold. Next, they sent out this code to tens of thousands of customers in the guise of a software update, which appeared to be perfectly legitimate, and the customers downloaded the 'update', only to have unwittingly granted the hackers access to their systems.

The sophistication of the attack and the effectiveness of its disguise meant it took well over a year to discover, during which time the hackers had unrestricted access to 18,000 customers' databases, and were installing additional malware into their systems.

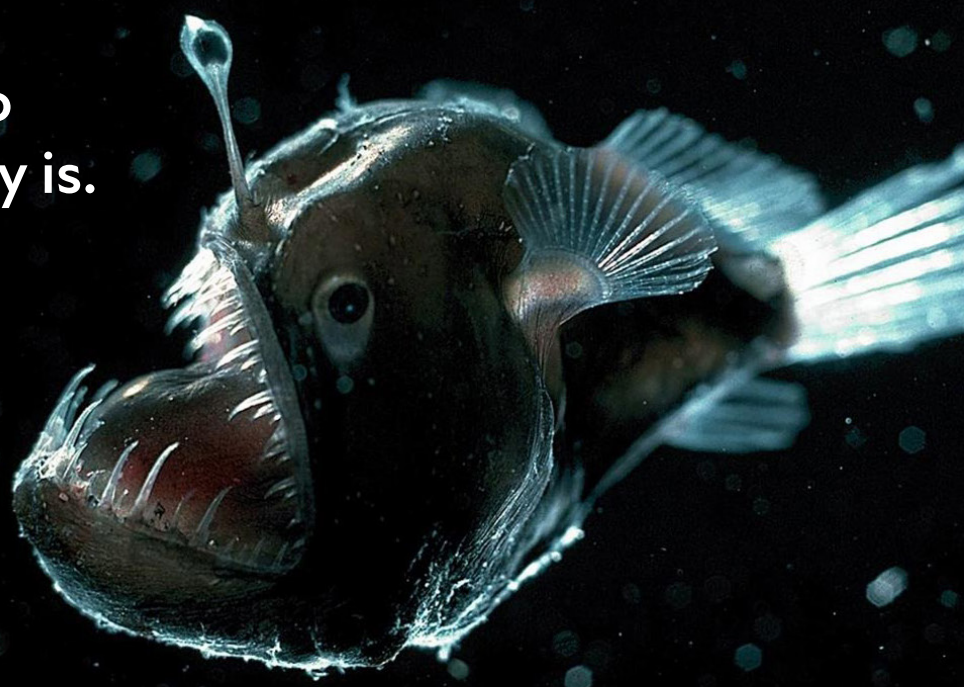
Stop it happening to you.

The best parasites are the ones the host doesn't notice, and it's especially difficult to recognise threats when they look like things you expect to see. Software updates from suppliers are commonplace, and (ironically in this case) installing them is part of cyber security best practice.

In the case of this software provider, it was nigh-on impossible for an average team member to spot, especially because it carried the correct digital signature. Education is the best defence – the trained eye can spot a fake software update.

Assuming that some of these attacks can or will fool someone, your organisation should of course monitor the system for malware, but also structure your systems and security measures so that one breach is less likely to infect or sabotage the whole company.

Lesson 2: When it seems too good to be true, it probably is.



FATAL ATTRACTION: Anglerfish tempt in smaller fish until they're close enough to swallow. Deep in the ocean, where there's no light, they use a bioluminescent fin ray as a natural lure.

In 2022, hackers stole $600m USD worth of cryptocurrency through the crypto-gaming platform that the currency underpinned.

It emerged that the hackers had gained access to the crypto platform through a sophisticated phishing attack, in which they approached a senior gaming engineer on LinkedIn about a fictitious job opportunity. The engineer completed several rounds of fake interviews, at the end of which he was offered a very generous salary – the 'offer letter' was a pdf that he eagerly downloaded, unwittingly admitting spyware into the system.

The hackers then managed to gain control of several 'validators' which validate transactions and authenticate ownership in blockchain and cryptocurrency networks.

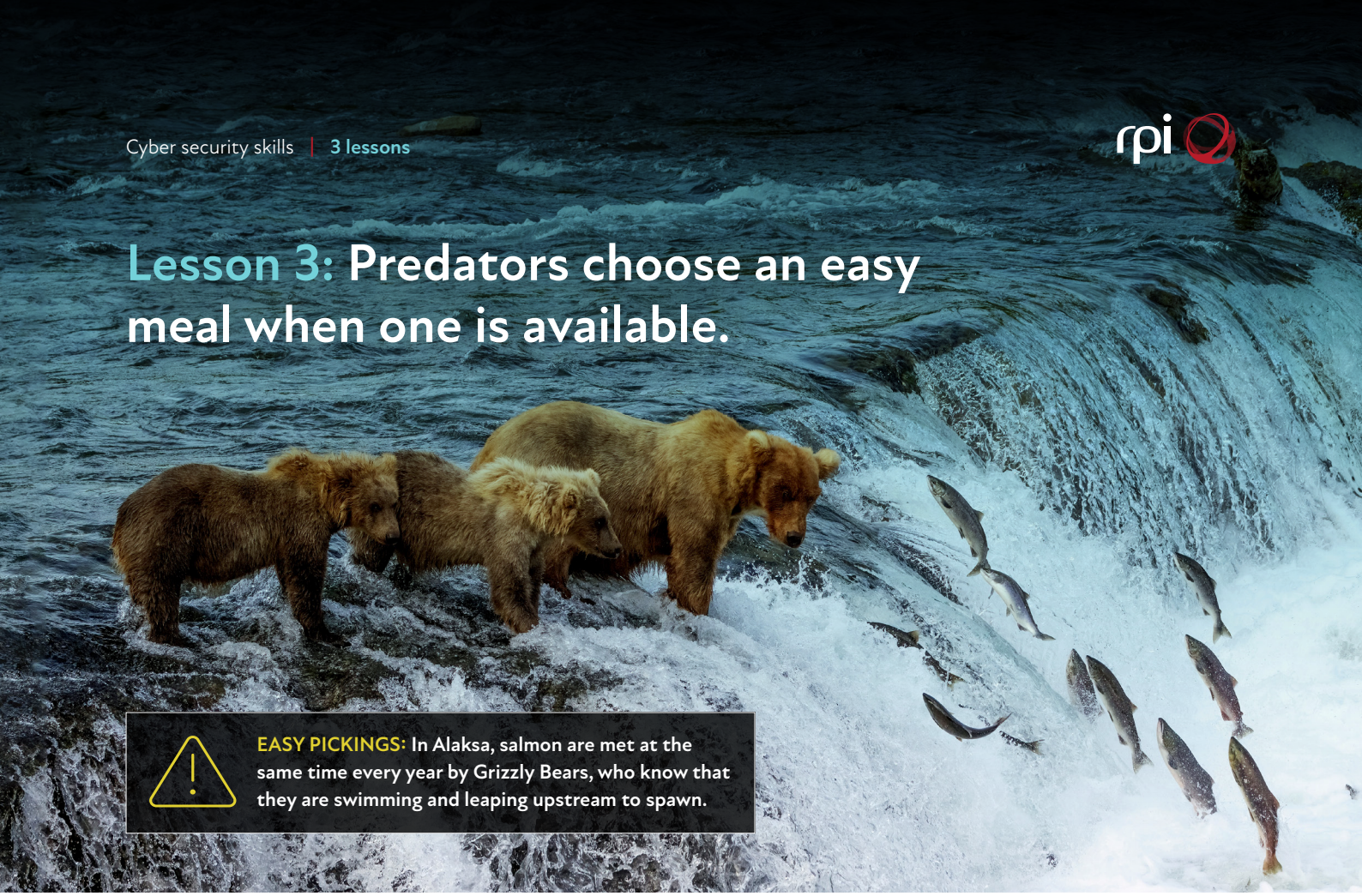
Stop it happening to you.

The brilliance of the attack is in its choice of disguise. Given that the exchange between the hackers and the victim was supposedly about a job at another company, the employee in question was extremely unlikely to discuss the messages with colleagues or bosses, and wouldn't encounter a second opinion as to whether the exchange was legitimate. There are two main ways to prevent this kind of breach:

- On a first and very basic level, institute a policy about personal files on company computers, forbidding downloads of personal or non-business files. It's by no means bombproof, but stands a good chance of deterring many instances of risky actions.

- Again, education forms a large part of the defence. It's not enough to print a policy in a handbook. Meaningful security education requires business leaders to communicate a message that will capture people's imaginations and lead to behavioural changes.

Lesson 3: Predators choose an easy meal when one is available.



EASY PICKINGS: In Alaksa, salmon are met at the same time every year by Grizzly Bears, who know that they are swimming and leaping upstream to spawn.

A major international provider of co-working space was discovered to have exposed data and documents from over 200 companies due to poor or absent Wi-Fi security. One user found that his fellow businesses' financial records were on full display on the network.

In this case, there was no 'attack' – data was there for the taking, and you can imagine that plenty got taken.

The revelation led to a massive devaluation for the co-working company and a hugely delayed IPO.

Stop it happening to you.

The short answer is to have security measures. In truth, things are far more complex than that. Some security is relatively weak or inappropriate for your company, so might offer a false sense of security, or be as good as having no protection at all. It might cover some parts of the business very well, but not others. It might simply be outdated, so that hackers know or can find easy ways through it.

In order to remain truly protected (and indeed to protect your customers), you need security leaders who:

- are familiar with (or even driving) developments in cyber security
- understand your sector and organisation deeply, and understand fully the strength and types of measures required
- are commercially aware, so that they appreciate and communicate the impacts of security breaches in a way that will secure the buy-in of C-suite and departmental managers.

One measure to repel all attacks.

Your business can't rely on attacks happening to other organisations – **you need experts** who can anticipate threats, not learn about them after the fact and hope your business doesn't become a lesson to others.

Cyber security has to be part of the fabric of the business, not a bolt-on or an afterthought. Organisations need people who know how to keep a growing business safe, while keeping it commercially viable and appealing to work for.

RPI specialises in placing exactly those people. The breadth of our network and depth of our sector expertise means that we're uniquely equipped to find the individuals to fit your business, and the talent to fill cyber security gaps in your leadership.

Email us now | Visit our website