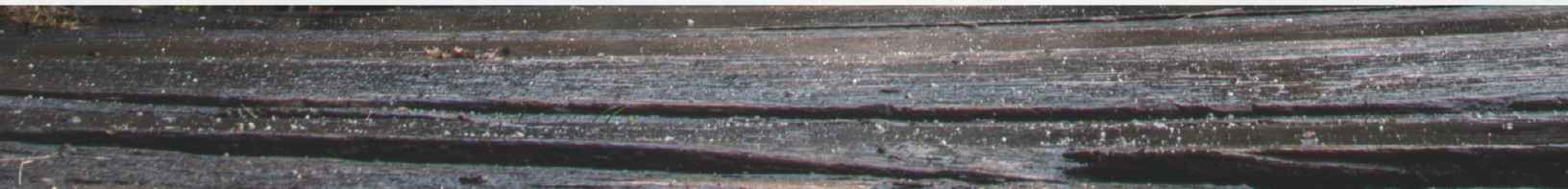
DYOPATH

# TEAR DOWN THE CASTLE

## A NEW APPROACH TO CYBERSECURITY FOR THE MODERN AGE



It's tough to think of an industry that changes more rapidly — and with higher stakes — than cybersecurity. In the last half-decade alone, the cybersecurity landscape has changed almost beyond recognition. Strategies that were accepted as no-brainers five years ago are dangerously ineffective today.

To survive in the minefield of cybersecurity threats that is 2024, organizations need to take a different approach to what worked in the past. You need to understand the new status quo, the new vulnerabilities, and the new strategies and techniques to survive.

To write this white paper, DYOPATH partnered with managed SIEM service ArmorPoint to give you an overview of today's cybersecurity landscape and share the strategies you need to implement strong, effective, layered cybersecurity in 2024 and beyond.

We'll hear from John Crowley, a Senior Account Executive and Partner Development Manager at ArmorPoint, and Sam Bourgeois, Director of Cybersecurity Services for DYOPATH.

## The Castle Analogy — Why Traditional Cybersecurity Is Obsolete

There's an old analogy in cybersecurity, one that you might have heard before. It goes like this — your organization is like a castle. In the same way that a castle has a moat, drawbridge, and towering walls to keep its occupants safe, your business has a complex and layered cybersecurity strategy to keep the bad guys safely outside.

All you need to do is keep your defenses strong so you can let the right people and data in, and keep the dangerous stuff out. And for many years, this was a great way to look at cybersecurity. Today, however, it doesn't quite cut it.

The main reason for this is remote work. Between 2019 and 2023, the percentage of employees worldwide who work from home all or most of the time went from 10% to 28%. Protecting your fixed "castle" with perimeter-based security is no longer enough — you need to protect your employees wherever they are, on whatever devices and networks they use.

This calls for a new approach to cybersecurity, one which we'll lay out and explain in the rest of this white paper.

## The Four Components of Modern Cybersecurity

How can today's businesses approach cybersecurity given the radically different set of circumstances and challenges they face?

We can break this new approach down into four key components.

## Risk-Based Cybersecurity

According to John, "Risk-based cybersecurity is focused on identifying, assessing, and prioritizing risk to an organization's most critical assets based on the potential impact of the likelihood of any threat."

This is such a fundamental idea that it's often overlooked or taken for granted. Without a strong understanding of the risks facing you and a clear strategy for dealing with them, you're essentially shooting in the dark.

To adopt a risk-based approach to security, start by taking inventory of all your assets, beginning with data and working up to software and hardware. Try to prioritize assets according to criticality, importance, and risk, and think about your network as a whole rather than a collection of disparate assets.

In the world of remote work, the risk-based approach is essential. When your assets are distributed outside your organization, you need to be aware of where they are and the risks they face at all times.

So how do you adopt a risk-based approach to cybersecurity? Here are some starting points:

- Make time for regular conversations within your organization about risk. Talk to your teams — not just security teams — and give them the means and channels to raise concerns easily.
- Create a risk register based on the reports from your team members and your risk analyses. Monitor this risk register on an ongoing basis and update it as often as possible.
- Take a data-driven approach. For example, use the data available for your market and industry to categorize and prioritize the risks in your risk register and make your teams as aware and informed as possible.

Risk-based cybersecurity is dependent on reliable data, which brings us neatly to the next key component of modern security.

## Data-Driven Cybersecurity

Data-driven cybersecurity uses analytics, machine learning, and AI to learn as much as possible about the threats facing your organization and to detect and respond to those threats in real time. A successful approach here relies on data from many different sources, including both your internal environment and external sources.

This type of security is effective because it adapts dynamically to threats as they emerge, and is based on the constant analysis of data patterns. This is a stark contrast to the old "castle-based" approach to security that relied heavily on static defenses and monitoring based on fixed rules.

Sam says, "I can tell you about so many examples where I've had organizations who are just rock solid in terms of perimeter and protecting the endpoint, even for the work at home and the hybrid. But they have no collection mechanism, and they're not looking for things that are already in the network, already on the system."

The more data you can collect, the better. You should be able to identify your top threats, create threat models, and be as informed as possible about what the data you collect means for your security and your organization.

## User-Focused Cybersecurity

The days of your users sitting safely in your castle, protected by a well-defended perimeter, are gone. Today, your users are out in the world, sitting in Starbucks, connecting to public WiFi networks from their personal devices. This exposes you to entirely new worlds of risk.

User-focused cybersecurity is an answer to this new status quo. It places the user — not the technology or infrastructure — at the heart of your cybersecurity strategy. For example, if your company has a bring-your-own-device (BYOD) policy, you absolutely need to have measures in place to prevent your users from accessing their email via standard clients, which have their own vulnerabilities.

Sam says, “User-focused, to me, means a targeted, thoughtful, well thought out and tested security program that puts humans in the middle and puts human tendencies and behaviors in the front and center.”

This all relies on a solid and reliable measuring strategy. It’s important to carry out penetration testing and carefully measure the effectiveness of your awareness training and simulation work to gain insights into your users’ behavior and level of preparedness. This allows you to build your security around keeping individual users safe wherever they are and whatever they’re doing.

### Compliance-Forward Cybersecurity

Complying with the right laws and regulations is an increasingly important part of cybersecurity in the modern world. Today’s organizations have more rules to be aware of and comply with than before. Many companies, however, treat this as a box-checking exercise rather than a central part of their security strategy.

John says, “Compliance-forward cybersecurity is an approach that integrates your regulatory compliance requirements into the core of an organization’s cybersecurity strategy, not the other way around.”

People will often ask, “How do we satisfy these requirements?” but that’s the wrong question. It focuses on doing the bare minimum to meet compliance needs, but the bare minimum is not where you should be aiming. Instead, focus on building a comprehensive security strategy that meets everyone’s needs and actually keeps the company safe — and you’ll likely fulfill your compliance requirements anyway.

## How to Build a Bespoke Cybersecurity Strategy

If you want to survive and thrive in today’s cybersecurity landscape, it’s no longer sufficient to take a cookie-cutter approach to security. You need a bespoke strategy that takes your specific, unique needs and challenges into account.

This kind of approach isn’t easy, but it becomes simpler if we break it down into some core goals.

### Protect the Business

Protecting the business goes back to the original castle analogy and the traditional approach to security. While this is no longer enough, it’s still important to consider your business as an entity and how to keep it safe.

This involves round-the-clock monitoring, drawing on tools like firewalls and cloud security posture management. Like the old approach, this relies on protecting your business with cybersecurity layers and strong virtual barriers, but it’s more complicated and nuanced.

### Protect Your Remote & Mobile Users

In 2024, the princess has left the castle. In other words, your business environment might be well-defended, but your assets and networks are being accessed from external locations and devices.

This demands a different approach. You need to focus on users and provide tailored, purposeful training and awareness programs that reflect your specific risks and challenges. You need to set clear expectations and rules and make sure your employees are aware of these requirements through ongoing training and clear, easily accessible materials and information channels.

It’s important to remember that most of your users aren’t security professionals, which means they simply aren’t aware of many of the risks involved in working from personal devices and public locations. It’s your responsibility as security experts to keep them informed and aware of the risks and how to keep themselves safe.

## Protect Your Data Everywhere

Ultimately, the bad guys targeting your organization are after your data. You need to guard this resource at all times, from every possible angle. Again, this comes down to layered security — not just around the perimeter of your organization but also for each individual user and around the data itself.

This means you need file encryption, data loss prevention solutions to track your data and monitor where it is and where it's going at all times, and immutable backups for all your data.

## Protect From Ransomware

Ransomware is one of the biggest threats facing companies of all kinds today. In a recent survey, 62% of businesses said ransomware is the number one concern for their C-suite, which represented a significant increase from 2022.

And these fears aren't unfounded. 2023 saw 317.9 million ransomware attempts globally, with the average cost of a successful attack reaching $5 million.

When a ransomware attacker gains access to your systems, they'll exfiltrate your data, destroy your backups, and encrypt your systems. After you pay the ransom — or don't pay the ransom — to regain access, they'll tell you they exfiltrated your data and demand yet another payment so they don't leak it.

File encryption is one of the best things you can do here, rendering any exfiltrated data worthless to an attacker. Immutable backups give you a lifeline if attackers attempt to destroy all your files. Data loss prevention and role-based access control help prevent and mitigate insider threats.

Ultimately, defense against ransomware is all about putting multiple layers of security in place based on your risk profile, risk tolerance, and the value of your data.

## Tearing Down the Castle & Tying It All Together

The castle analogy is no longer an appropriate way to think about cybersecurity. "Let's tear down the castle," says Sam. "We're not trying to update the castle. We're never going to be able to build a castle in modern terminology."

You need to stop thinking about cybersecurity as a destination and start thinking about it as a journey. This is because you can never eliminate risk. There's always a risk that one of your team members will fall victim to a phishing scam, leave their laptop on the subway, or turn out to be a criminal themselves.

The solution is not to remove all risk but to prepare as best you can. Determine your risk profile, get familiar with all the threats facing your organization, do everything you can to protect all your users and assets, and be committed to continuous improvement and adaptation.

There is no one-size-fits-all model here. John says, "It's about the type of business that you have and where the data ultimately lives. And so it really does come down to understanding the core business and what that looks like."

## Work With DYOPATH

At DYOPATH, security is a central part of our managed services offering. We help businesses of all sizes adapt to the new era of cybersecurity and protect their users, assets, and data wherever they are from all kinds of threats.

Security services are included in our overall suite of managed services, and we also have DYOGUARD — a product specifically focused on managed cybersecurity services, which you can learn more about here.

**If you want to find out more about DYOPATH, what we offer, and how we can help you remain safe and prepared in the modern cybersecurity landscape, schedule a call with us.**

### If you want to learn more . . .


Visit our Website


Call us at (866) 609 - PATH


Email us at solutions@dyopath.com