DYOPATH

The IT Director's Blueprint for IT Maturity

In a world that's more competitive and tech-dominated by the day, businesses no longer have the option of ignoring their IT maturity.

Those who take the time to invest and prioritize their IT stand to gain a powerful competitive advantage, while those who neglect this area risk being overtaken.

It's now widely acknowledged that more mature organizations tend to perform better across multiple metrics. For example, research by Deloitte found that 45% of high-maturity companies reported a net revenue growth significantly above industry averages, compared to just 15% of companies with lower maturity.

There are many reasons to prioritize greater IT maturity, but the process of getting there is not easy and requires a multi-pronged, sustained approach.

The journey to IT maturity is one that will last a lifetime. There is no finish line — it's a constant process of analyzing, building, and upgrading.

DYOPATH CIO James Melchor understands more about IT maturity than most. We spoke to him to get his thoughts on what organizations — and IT directors in particular — can do to build more mature and successful companies.

In this white paper, we'll share Melchor's insights along with a blueprint for IT directors to follow when it comes to achieving and maintaining IT maturity, outlining and exploring several key areas to focus on.

Established Processes

According to Melchor, a central part of IT maturity is having the right processes firmly established in all relevant areas.

Think about processes like incident management, crisis management, request management, and so on. This allows you to catalog events and critical items coming into the environment, and gain a deeper understanding of the organization as a whole.

Established Processes — What's at Stake?

Low-maturity companies often don't track anything at all, since they don't have the right processes and mechanisms in place to track. This leads to many serious risks:

- **A lack of standardization when it comes to handling incidents.** As a result, in times of crisis, you have no established response in place, leading to a disorganized scramble to solve serious, time-sensitive problems.

- **A lack of visibility into recurring problems.** This means when problems reoccur, you don't have critical insights into the root causes of the issue and are forced to keep fixing the symptoms rather than the deeper factors. It's the IT equivalent of spending all day swatting mosquitos instead of simply closing the door and keeping them out.
- **A negative perception of IT.** Without established processes, your IT teams can quickly develop a reputation for being unreliable and inefficient, eroding their relationship with the rest of the organization and making it even more difficult to maintain visibility in key areas.

Overall, a failure to establish and maintain processes can have a profoundly negative impact on efficiency, quality, worker morale, and outcomes in a wide range of areas in IT and beyond.

How to Establish Processes

The first step to establishing the right processes is to carry out an evaluation.

What are you doing right now? Do you have any ITIL-aligned core processes in place at all?

If so, assess each process in turn — how well designed is it, and how well evaluated is it on a continual basis? This is a good starting point for building stronger, more sustainable processes throughout your IT infrastructure.

Here is a checklist of key established processes to put in place.

○ Incident Management

○ Crisis & Major Incident Management

○ Problem Management

○ Service Request Management

○ Self-Service Request Management

○ Knowledge Management

○ Change Management

○ Continuous Improvement

○ Service Level Management

○ Access Management

○ Availability Management

○ Capacity Management

○ Event Management

End-User Support Functions

End-user support functions include—at a bare minimum—user support, end-user multi-factor authentication, endpoint disk encryption, and management of endpoint devices.

These functions are absolutely essential from an IT perspective. You'll also need to consider third-party patching, endpoint detection and response on all relevant devices, and security around communication channels like email. If you don't have these processes in place, there's a lot at risk.

End-User Support — What's at Stake?

Without the right end-user support functions in place, your data will be more vulnerable.

"Your end-users are some of your most susceptible entry points for risk," says Melchor. "So you need to have the right support tools at the endpoint or end-user level, and be supporting and managing those to ensure that you're not susceptible to compromise."

This is extremely serious due to the high relevance and importance of data for modern organizations, and the need to protect data not only for your own security but to comply with ever-stricter privacy regulations.

Weak end-user support can also threaten your overall business operations due to poor support and reduced productivity. When your organization appears unreliable, disinterested, and incompetent, your brand will suffer.

How to Improve End-User Support

The first step, as always, is to carry out an assessment to find out what end-user support and security functions you already have in place.

If it turns out there is no — or very little — standardization around your services in this area, it's time to make some changes. Start by locating your most vulnerable areas and begin building them up.

Here is a checklist of important end-user support functions.

Share this with your teams to make sure you are building the right processes to drive greater IT maturity.

- ○ Service desk and end-user support
- ○ Multi-factor authentication (MFA)
- ○ Endpoint disk encryption
- ○ Managed endpoint management
- ○ App management
- ○ Policy deployment
- ○ Self-service features
- ○ Windows Autopilot
- ○ Windows Autopatch
- ○ Disk encryption management
- ○ Endpoint patching
- ○ Endpoint 3rd party patching
- ○ Endpoint Detection and Response (EDR)
- ○ Email and collaboration security
- ○ Email security detection and remediation
- ○ Protection for Microsoft Teams
- ○ Social engineering defense
- ○ Insider risk protection
- ○ DMARC management
- ○ Message encryption
- ○ Email continuity

Infrastructure Support Functions

The state of your core infrastructure and how it's managed will have a huge bearing on your overall security, productivity, and efficiency.

Core infrastructure encompasses things like your servers, storage, networks, cloud applications, and virtual machines. The relevant functions here include encryption, third-party patching, network patching, and endpoint detection and response.

Infrastructure support functions are similar to end-user support functions, but they take place at the infrastructure level of your company. It's the difference between a single device being impacted and the entire email system being down.

Infrastructure Support — What's at Stake?

Failing to invest in your infrastructure support comes with significant risks. Here are some of the key threats that can result here:

- **Connectivity issues.** Poor infrastructure support can lead to slow, unreliable network connections across your organization, especially at remote sites. This in turn can massively impact productivity and slow down your business processes. Research suggests that 85% of SMEs say their productivity is impacted by an unreliable internet connection.
- **Compromised data.** Without the right infrastructure in place, you'll suffer more vulnerabilities, increasing the likelihood of bad actors accessing data that's critical to your business operations and stability.
- **Poor performance.** Insufficient infrastructure leads to slow, unreliable, and problem-prone applications, causing major issues at all levels of the organization.
- **Alerts not being monitored.** Failing to keep on top of key alerts can lead to breakdowns in communication and missing key information, which can take a heavy toll on productivity.

How to Improve Infrastructure Support

Improving infrastructure support involves a number of key intersecting tasks. Start by assessing what functions you currently have in place and which areas need to take priority.

Here is a checklist of key infrastructure support functions.

Use this checklist with your teams to make sure you are taking steps in the right areas when it comes to reaching maturity in infrastructure support.

○ Managed infrastructure

○ Server

○ Virtual machine

○ Storage

○ Network

○ Cloud

○ SaaS

○ Infrastructure desk encryption

○ Infrastructure patching systems

○ Infrastructure 3rd party patching systems

○ Infrastructure patching network

○ Endpoint Detection and Response (EDR)

Security

Security is an enormously important factor in IT maturity and should be a key point of focus for any IT director.

In fact, security is one area that extends far beyond technology. A Gartner study found that 88 percent of Boards of Directors (BoDs) view cybersecurity as a business risk as opposed to a technology risk.

Understanding the vulnerabilities within your organization and taking concrete steps to address them is essential, and failing to do so can carry fatal consequences for your business. IT directors need to ensure their approach to security is up-to-date, backed by the right technology, and adaptable.

Security — What's at Risk?

The list of potential risks when it comes to organization security is almost endless, and new threats emerge on an ongoing basis.

One risk is compromised revenue. For example, organizations can be coerced into sending large sums of money to what they believe is a vendor's bank account but is actually a criminal operation.

Such events can severely damage companies from a revenue and brand perspective, even if they only happen sporadically.

> *"Security is massively impactful from the standpoint that compromising of data, compromising stolen revenue… these things are more extremely impactful from a revenue and brand perspective. These can crater companies."*
>
> — James Melchor, CIO, DYOPATH

How to Improve Security

The first stage of improving your security is to focus on gaining a clear overview of your organization and endpoints — to understand all the data coming from your end-user devices, applications, and network infrastructure. This visibility allows you to quickly identify any vulnerabilities and risks and take decisive action.

The next stage is to start running tests to assess how your security infrastructure might fare in a real attack. Red Teaming is one of the best methods here, where specialists run a simulated attack on your systems to ensure your security apparatus is capable and to highlight any areas of weakness.

Here is a checklist of key security areas.

Use this checklist with your teams to make sure you are doing exactly the right things when it comes to building a secure and mature organization.

○ Vulnerability management

○ Security Information and Event Management (SIEM)

○ SOC-as-a-Service (SOCaaS)

○ Security awareness training

○ Red Teaming-as-a-Service (RTaaS)

○ Virtual CISO (vCISO)

○ Compliance Operations-as-a-Service (COaaS)

DYOPATH's Approach

At the beginning of this white paper, we talked about how IT maturity is a continuous journey. This means that continuous improvement must be built into your approach, with a focus on monitoring, updating, and improving.

To build and maintain a culture of continuous improvement, here are some best practices to follow:

- **Establish key metrics to track**. You'll need to pay attention to the right key performance indicators. These can be technical like network latency, server uptime, and number of security incidents, or things like customer satisfaction scores and return on investment. Tracking the right metrics allows you to monitor progress and quickly identify areas of concern.
- **Carry out standardized evaluations.** Evaluations are the best way to assess your IT maturity and work out what needs to change in order to keep improving. These assessments should be standardized to ensure the same approach is followed each time.
- **Frequency is key.** It's essential to regularly review your IT maturity to make sure things are on track and make any course corrections. This includes the evaluations above, as well as team meetings, reports, and possibly third-party assessments.

The main question you should always be asking when it comes to every element of IT maturity is, "Is this meeting my business requirements and needs?"

Is your current set of tools, processes, and functions helping your organization get to where it needs to be? Asking these questions regularly and thoroughly seeking out the answers are some of the best things you can do for your IT maturity.

> *"Much like security is a journey and not a destination, IT maturity is definitely a journey and not a destination."*
>
> — James Melchor, CIO, DYOPATH

Don't Go It Alone

For best results with IT maturity, IT directors need a guide. With the help of an experienced third-party team, it's much easier to identify problems and make consistent progress.

Think of it like maintaining a house. When you spend all your time inside the house, it's difficult or even impossible to notice certain issues. You need a building inspector and a contractor for major jobs, and a handyman for smaller, day-to-day jobs.

The same applies to your IT maturity journey. An external team can help pinpoint issues your own teams might miss. They can help you zoom out and make key decisions in the context of your competitors and the longer-term environment of your industry. The right partner can also help you handle the compliance element of IT maturity to ensure you remain on the right side of existing and emerging regulations.

Work with DYOPATH

At DYOPATH, our team of experts is well-positioned to help you achieve your IT maturity goals and build a sustainable system to serve your needs.

Our suite of managed services can help you take care of everything from security and connectivity to cloud services. We'll guide you through regular assessments to diagnose areas for improvement and implement key changes to your infrastructure.

If you want to take your IT maturity to the next level by plugging into the wealth of advantages that come with professional managed services, contact us today!

If you want to learn more . . .

Visit our Website

Call us at (866) 609 - PATH

Email us at solutions@dyopath.com