#RSAC

RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **PART3-T08**

Targeted, Consolidated & Coordinated Services for Better Risk Reduction

Robert Fink

Principal Consultant / vCISO
BlackBerry Strategic Services

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

The Acceleration of MSSP and Cloud Adoption

- Work from home and the “Great Resignation” helped accelerate the adoption of managed security services providers (MSSPs)
  - Market growth was already increasing due to increasing regulations, rising security breaches, and the already tight cybersecurity talent pool
  - The global MSS market size is projected to grow from USD 22.8 billion in 2021 to USD 43.7 billion by 2026, at a Compound Annual Growth Rate of 13.9%

https://www.bloomberg.com/news/articles/2021-05-10/quit-your-job-how-to-resign-after-covid-pandemic

https://www.reportlinker.com/p05749258/Cloud-Computing-Market-by-Service-Deployment-Model-Organization-Size-Workload-Vertical-And-Region-Global-Forecast-to.html?utm_source=GNW

The Acceleration of MSSP and Cloud Adoption

- In some organizations the rush to address these challenges with MSSPs came at the expense of resourcing/risk in other areas
- In many cases we saw organizations overcompensating with new tools and services in the areas of Detection and Response at the expense of their Identification, Prevention, and Recovery strategies

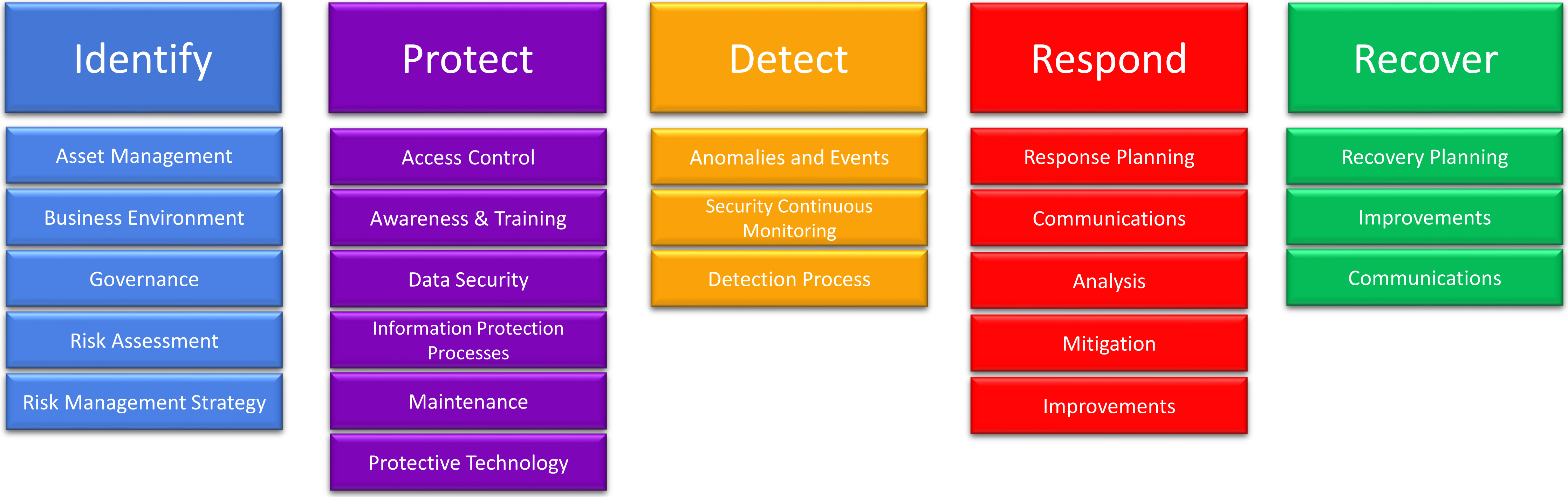
Does this sound familiar? How do you fix it?

- A full, programmatic gap assessment can help to recognize and correct the imbalance and guide not only the redistribution of resources, but also your MSSP strategy going forward
- This type of assessment can help identify under-resourced areas and provide a roadmap for targeted moves to rebalance and reduce risk
- With the help of the right MSSP partners, you may be able to better consolidate and coordinate services and achieve additional risk reduction

Where do you start?

- Start with an assessment of your requirements
  - Areas that have clearly been neglected
  - Areas currently under-resourced with too much risk
  - Areas where there is a clear skills gap
  - Areas where you may have overlap in existing tools or services
  - Areas where it may not be feasible or advisable to resource internally
- Consider using a security framework to guide your review
- Compare the findings to your deployment of tools and MSSP services

What might this type of assessment look like?

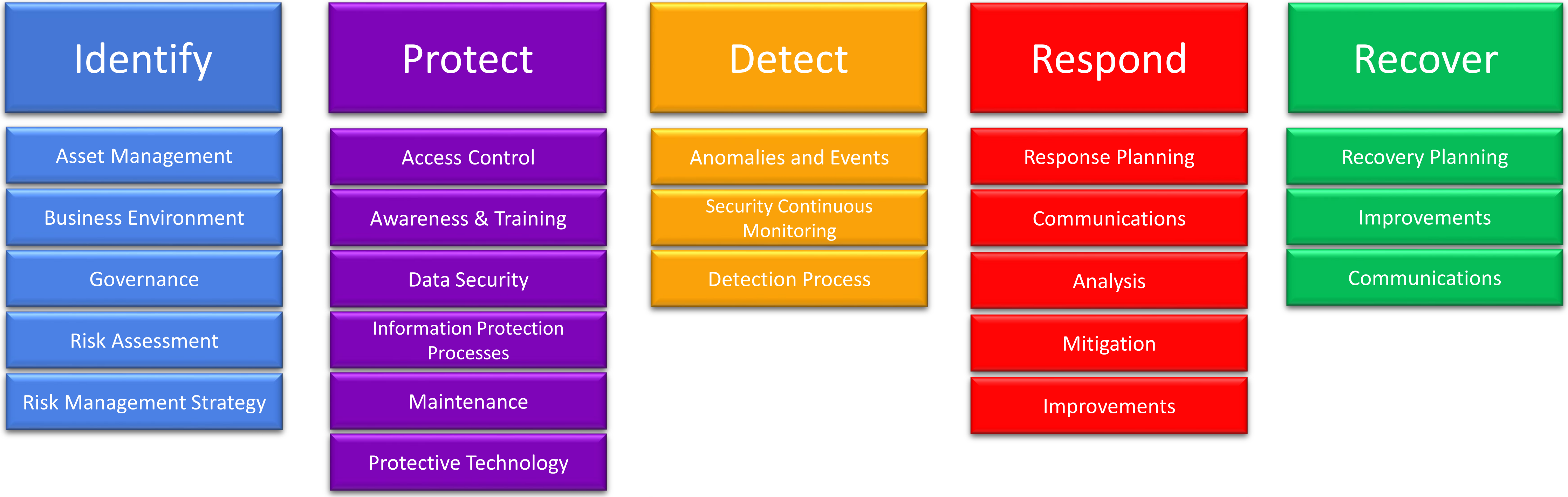


Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness & Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Process	Analysis	Communications
Risk Assessment	Information Protection Processes		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

https://www.nist.gov/cyberframework

Compare the findings to your deployment of tools and MSSP services

How can MSSPs provide the most help?



Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness & Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Process	Analysis	Communications
Risk Assessment	Information Protection Processes		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

https://www.nist.gov/cyberframework

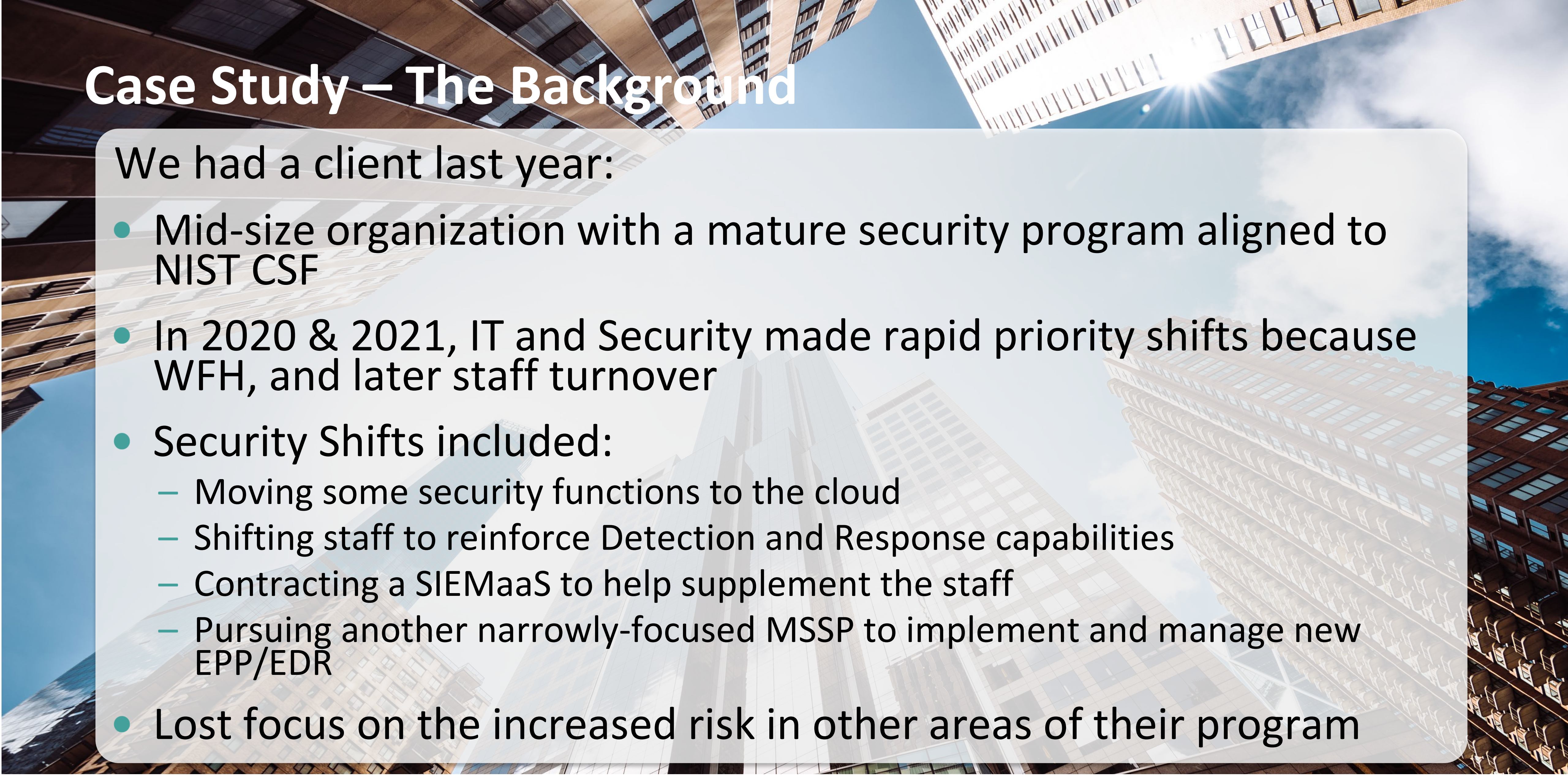
Narrowly-focused MSSP services
usually cover one or two areas

How can MSSPs provide the most help?

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness & Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Process	Analysis	Communications
Risk Assessment	Information Protection Processes		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

https://www.nist.gov/cyberframework

Full Spectrum MSSP Services can coordinate
and help orchestrate across multiple areas
… and become a force multiplier!



Case Study – The Background

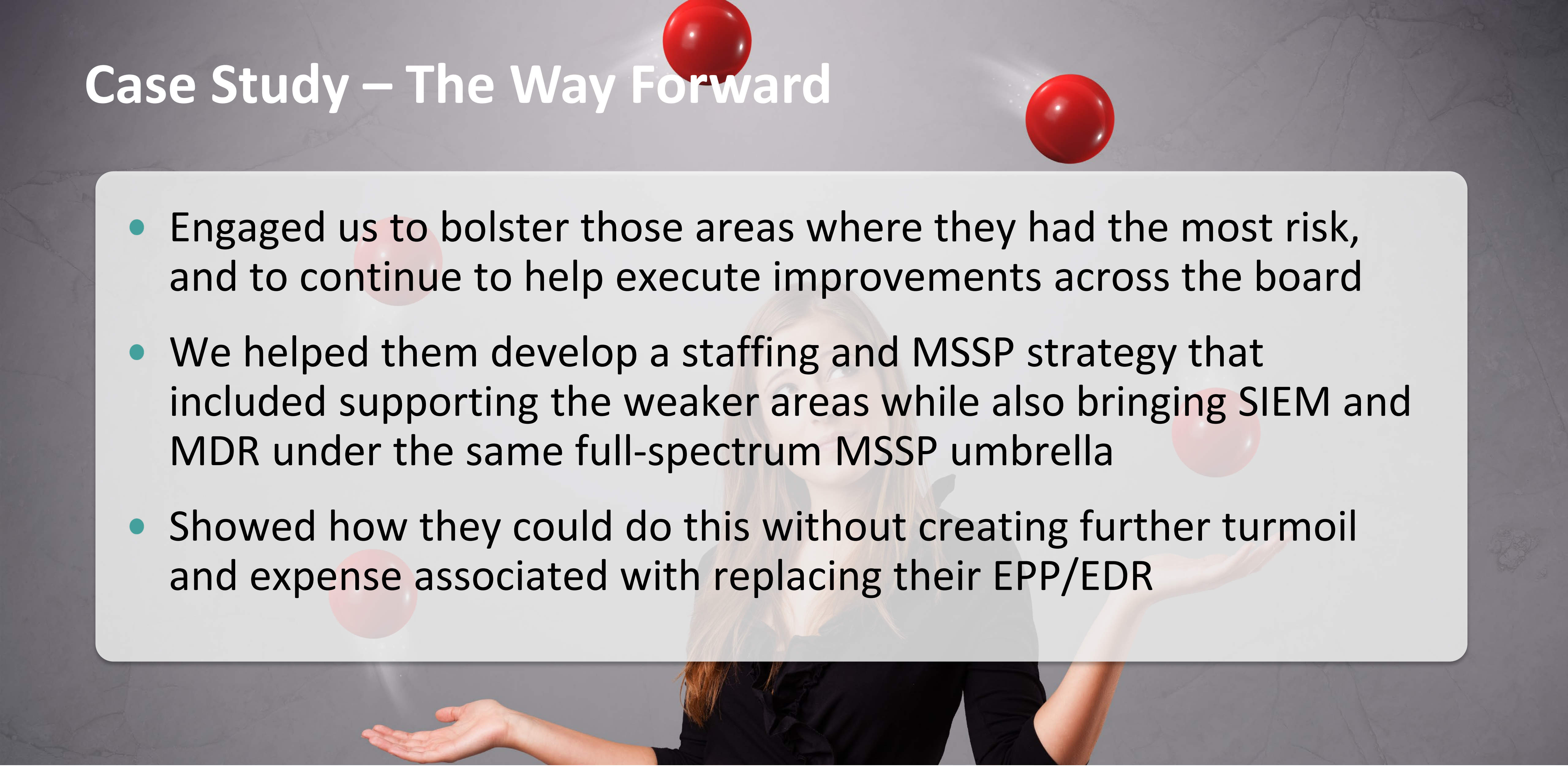
We had a client last year:

- Mid-size organization with a mature security program aligned to NIST CSF
- In 2020 & 2021, IT and Security made rapid priority shifts because WFH, and later staff turnover
- Security Shifts included:
  - Moving some security functions to the cloud
  - Shifting staff to reinforce Detection and Response capabilities
  - Contracting a SIEMaaS to help supplement the staff
  - Pursuing another narrowly-focused MSSP to implement and manage new EPP/EDR
- Lost focus on the increased risk in other areas of their program

Case Study – The Assessment & Findings

- Assessment revealed obvious gaps in the program, calling attention to the risks in: Identify Protect Recover
- Highlighted internal skill gaps in these areas requiring either additional staff, training, or more professional services
- Identified the probability of exacerbating the problem with their plans to bring in another narrowly-focused MSSP to “improve” EPP/EDR

Case Study – The Way Forward



- Engaged us to bolster those areas where they had the most risk, and to continue to help execute improvements across the board
- We helped them develop a staffing and MSSP strategy that included supporting the weaker areas while also bringing SIEM and MDR under the same full-spectrum MSSP umbrella
- Showed how they could do this without creating further turmoil and expense associated with replacing their EPP/EDR

How we were able to help

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness & Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Process	Analysis	Communications
Risk Assessment	Information Protection Processes		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

https://www.nist.gov/cyberframework

- **Current Risk & Security Control Assessment**
- **Governance Procedures**
- **Revised Resourcing Strategy**

- **IRP Training**

- **Retained EPP/EDR**

- **Added MDR w/ SIEMaaS**
- **Adding XDR/MXDR**

- **IRP & TTX**

- **Backup Assessment**

vCISO - Coordination & Orchestration

Keys to their Success

- Assessment of risk and controls
- Additional consideration of internal and external (MSSPs) resourcing
- Engaging a full-spectrum MSSP who:
  - Consolidated and improved Detection and Respond capabilities, without replacing existing EPP/EDR tools
  - Had a broad portfolio of services to also help in the areas of Identification, Prevention, and Recovery planning
  - Had a deep bench of analyst, engineers, and a strategic tier of principal consultants with years of experience leading and orchestrating security programs

Apply What You Have Learned Today

Next week:

- Conduct an assessment of your security program
  - Risk, controls, and resource utilization

In the first three months:

- Develop improvement roadmap

Within six months:

- Bolster weak areas, consolidate functions and resources where possible, attempt to lessen complexity and costs

Questions