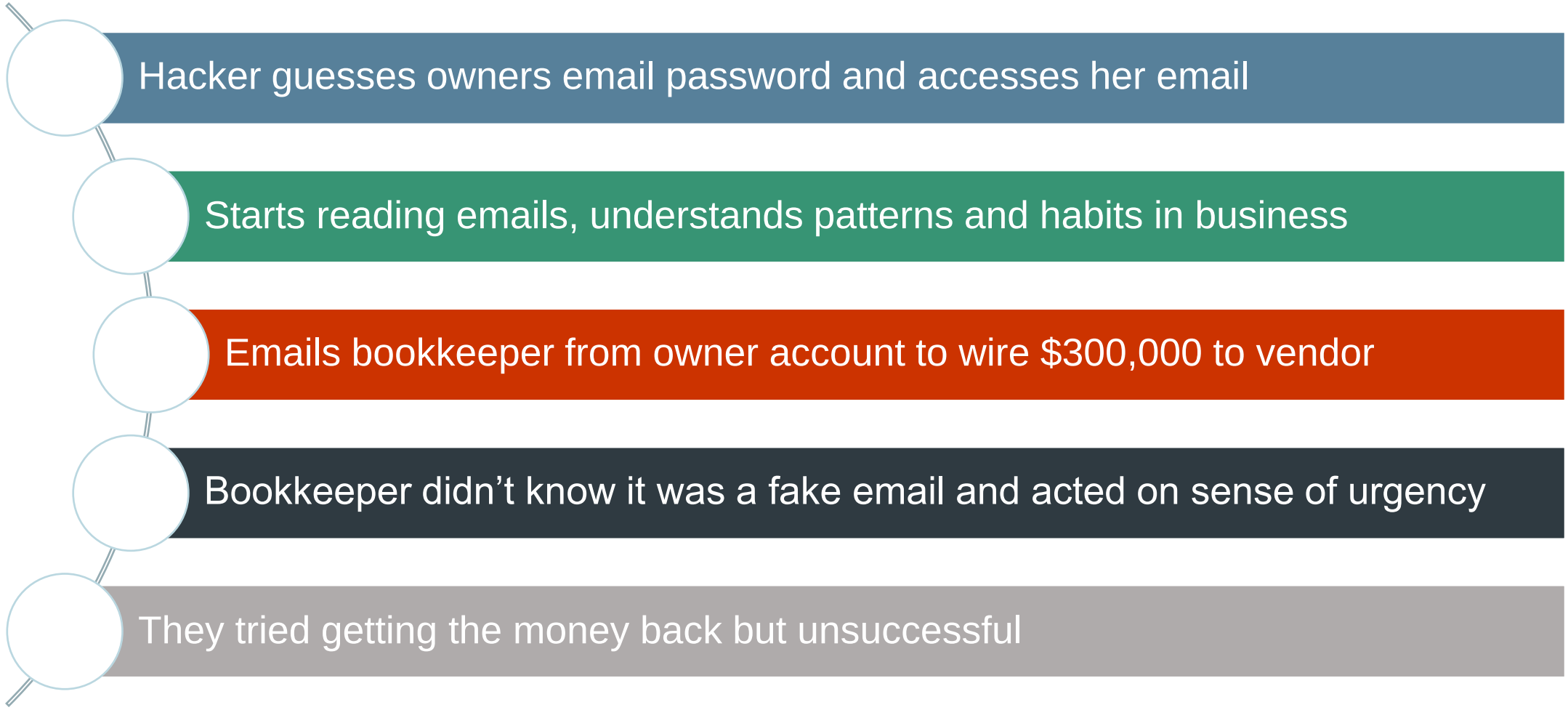
Every organizations must have IT plan for cybersecurity

Nikhil Jagga
President
njagga@cmitsolutions.com

How a small business owner lost $300,000



What mistakes did this owner make?

- Weak password – kid's name and zip code: "jennifer10598"
- No 2-factor authentication on accounts
- Use the same password for multiple accounts – bank accounts, insurance, amazon
- Exchanging sensitive account information via email e.g passwords, account numbers

5 simple things you can do today

- Change your passwords to be stronger – min length of 14
- Enable 2 factor authentication where available
- Delete password if you are storing them in browsers like Chrome
- Do not use the same password for multiple accounts – bank accounts, insurance, amazon
- Exchange sensitive account information via a secure communications tool

Medium Term

- Move beyond rudimentary safeguards and **implement 10-15 best practices**
- Continuous education for employees on security pitfalls but education isn’t enough
- Have employees demonstrate they understand how to act – test employees

What is driving this attack trend on small business computer systems?

- Things move too fast for an individual IT person or owner to keep up with
- Lack of time, budget, and security expertise
- Doing more with less
- **Hybrid work – home and office**
- **Sharing work computers with family**

Things you can do

Today

- Educate employees about keeping a separation between work and personal use of technology
- Consider increasing home security especially if you are in regulated industry – financial services etc
- Keeping all your devices updates with manufacturer recommended updates
- Make sure your data is backed up and tested

In next 2 weeks

- Implement layers of security, in case they get through one layer you have other layers protecting
- Get cyber insurance
- Have an incident response plan

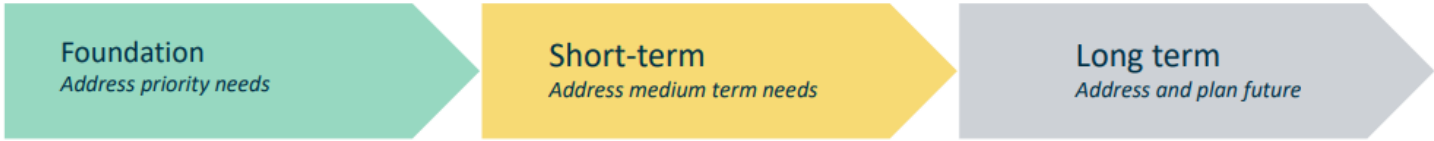
CMIT Look Back and Look Forward Approach

On Assessment calls

Look Back - State of Cybersecurity

	Issue	Score	Risk/Impact
1	We have conducted a Cyber Risk Assessment in the last 12 months from a reputable source		Compliance and ransomware
2	We monitor and update our computers regularly per manufacturers guidance	1	Ransomware, disruption, performance
3	We have the latest prevention, detection, response, and threat hunting antivirus software	0	Ransomware, disruption
4	We have MFA enabled on all cloud and non-cloud applications including network devices	0	Ransomware, disruption
5	Our data is regularly backed up, encrypted and monitored. We have tested restoring the data	1	Downtime and disruption
6	We conduct security awareness training for our staff weekly or monthly	1	
7	Our firewalls, switches and other equipment are monitored for active threats and kept updated with latest software updates	1	

Look Forward – Prioritized Risk based multi-layer IT plan



Set up your minute “assess your risk” call

njagga@cmitsolutions.com