

## Understanding Cybersecurity Breaches & the Estée Lauder Breach



Who & what was the potential target?

The type of Institution
What systems were targeted?
What was taken and how?
Who was responsible and who was affected?



What was impacted?

Impacts to production

The lost of time and since of security

Economical Impacts



How the breach was addressed & protecting systems from future threats

Securing the data
Understanding the vulnerabilities
Tools for securing data

### Understanding Cybersecurity Breaches & Threats

- There's no specific profile for a hacker
- There is no system that can't be hack
- With enough time and resources any system can be breached
- Access can be gained through:
  - Social engineering
  - Shoulder surfing
  - Scare tactics
  - Poor password creation
  - Poorly secured networks and device, etc.;



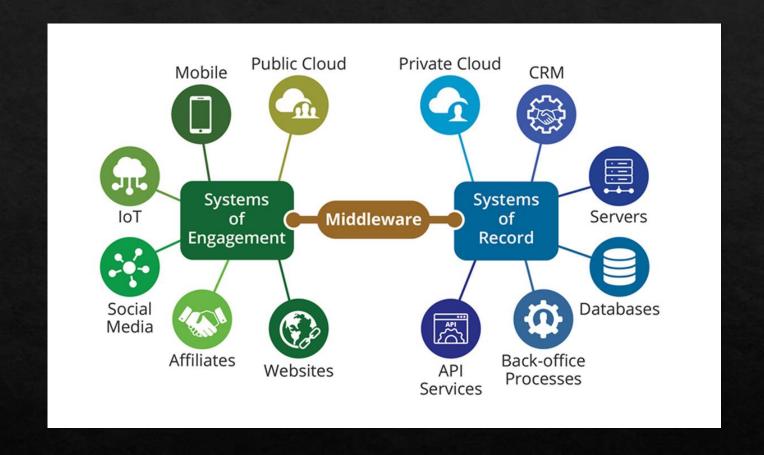
### Who & what was the potential target?

- International Fashion & Cosmetics Corporation
- Customers
- Employees
- Potentially clients & vendors
- Internal systems & networks

#### ESTĒE LAUDER

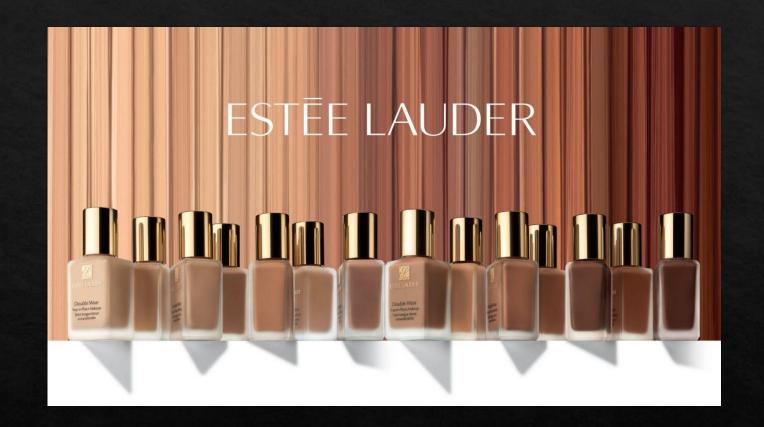
# Who & what was the potential target? Cont'd

- Middleware
- Data Management
- Application Services
- API management
- Messaging



#### What was impacted?

- Was there an impact on production?
- Was there an economical impact?
- Was there an impact to a since of security?



How the breach was addressed & protecting systems from future threats

- Securing the data
- Understanding the vulnerabilities
- Tools for securing data



# How the breach was addressed & protecting systems from future threats Cont'd

- Ways to secure systems and protect devices from future breaches
  - Secure password
  - Multifactor authentication
  - Biometrics (finger prints, voice, retinal, facial)
  - · Website security
    - VPN (Virtual Personal Network
    - DMZ (Demilitarized Zone)



### How the breach was addressed & how to protect our systems from future threats Cont'd

Additional security tools and practices:

- Monitoring systems
  - Solar Winds
  - Intruder
  - Syxsense
  - Acunetix
  - Wireshark

#### Cyber & data security best practices

- Require password changes every 60 days
- Require strong password
- Require the use of multi-factor authentication
- Require the use of a VPN to access network
- Use encryption when creating code
- Layered security

```
FaultPrevented()){var h=a(d);this.activate(b.closest("li"),c),this.activate(h,h.parent(), Tunccio
  rigger(\{type: "shown.bs.tab", related Target: e[0]\})\})\}\}, c.prototype.activate = function(b,d,e)\{function(b,d,e)\}\}
  active").removeClass("active").end().find('[data-toggle="tab"]').attr("aria-expanded",!1),
  ia-expanded",!0),h?(b[0].offsetWidth,b.addClass("in")):b.removeClass("fade"),b.parent(".dropdow
  ().find('[data-toggle="tab"]').attr("aria-expanded"
                                                                                                                                         c()}var g=d.find("> .active"),h=e&&
  /e")||!!d.find("> .fade").length);g.length&&h?g.one
                                                                                                                                             tionEnd",f).emulateTransitionEnd
                                                                                                                      bsTrans
  ;var d=a.fn.tab;a.fn.tab=b,a.fn.tab.Constructor=q
                                                                                                                                                 fonflict=function(){return a.fn.t
  "show")};a(document).on("click.bs.tab.data-api",
                                                                                                                                                  "tab"]',e).on("click.bs.tab.data
 se strict"; function b(b){return this.each(functi
 *typeof b&&e[b]()})}var c=function(b,d){this.opti
                                                                                                                                                 this),e=d.data("bs.affix"),f="ob
  ",a.proxy(this.checkPosition,this)).on("click.bs.affix.data-api",a.proxy(this.checkPositionWi
null, this.pinnedOffset=null, this.checkPosition()};c.VERSION="3.3.7",c.RESET="affix affix-top
State=function(a,b,c,d){var e=this.$target.scrollTop(),f=this.$element.offset(),g=this.$target.scrollTop(),f=this.$element.offset(),g=this.$target.scrollTop(),f=this.$element.offset(),g=this.$target.scrollTop(),f=this.$element.offset(),g=this.$target.scrollTop(),f=this.$element.offset(),g=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=this.$target.scrollTop(),f=t
"bottom"==this.affixed)return null!=c?!(e+this.unpin<=f.top)&&"hottom"
```

# In Conclusion, "What did the Estée Lauder breach teach us?"

- Threats can come from anywhere, even from human error
- The benefits of testing regularly for security vulnerability
- Make sure to properly secure all data, with added security for highly sensitive data
- Insuring the proper setup and security of middleware applications
- Using best practices for continual prevention of breaches and attacks



#### Work Cited

#### References

Lane, A. (n.d.). Strategies For Protecting Web-Facing Databases, Dark Reading, 8AD. Retrieved from Darkreading.com: https://www.darkreading.com/risk/strtegies-for-protecting-web-facing-databases/d/d-id/1138203

Series, C. S.-O. (20, April 5). Introduction - OWASP Cheat Sheet Series. Retrieved 2021, from https://cheatsheets.owasp.org:

https://cheatsheetseries.owasp.org/cheatsheets/Cross\_Site\_Scripting\_Prevention\_Cheat\_S heet.html

Winder, D. (2020, February 11). "Estée Lauder Database Exposed, Customer Data Not Involved" Forbes". Retrieved from Forbes.com:

https://forbes.com/sites/daveywinder/2020/02/11/estee-lauder-data-leak-440-million-records-exposed/?sh=3b4901832590