INFORMATION SECURITY UPDATE

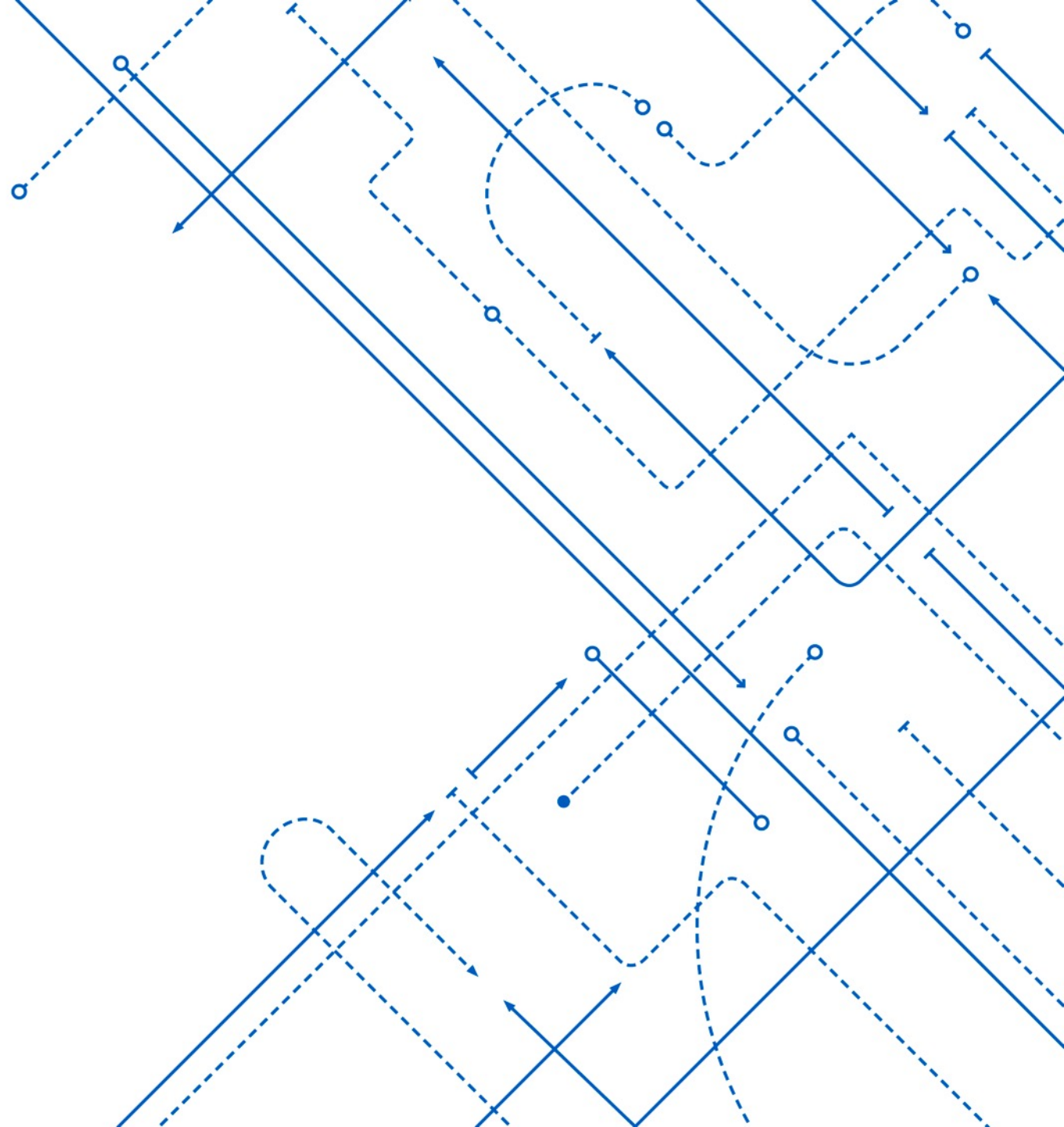
ISO 2019 Summer Plans and Direction

University at Buffalo
Information Technology

THE ISO

Information Security Office

University at Buffalo
Information Technology



The Practice of Information Security

Two main divisions of professional practice in the ISO

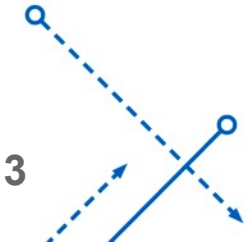
- Security Operations (SecOps): “Technical” security controls (plus “physical”)
- Risk & Compliance: “Administrative” security controls
- (Plus everyone does Response, TEA, Office functions, etc.)

SecOps examples

- SIEM, vulnerability scanner, firewalls, anti-virus, penetration testing tools, 2-factor authentication, remote access gateways, IDS/IPS, login IDs and passwords, data recovery/forensics, etc.

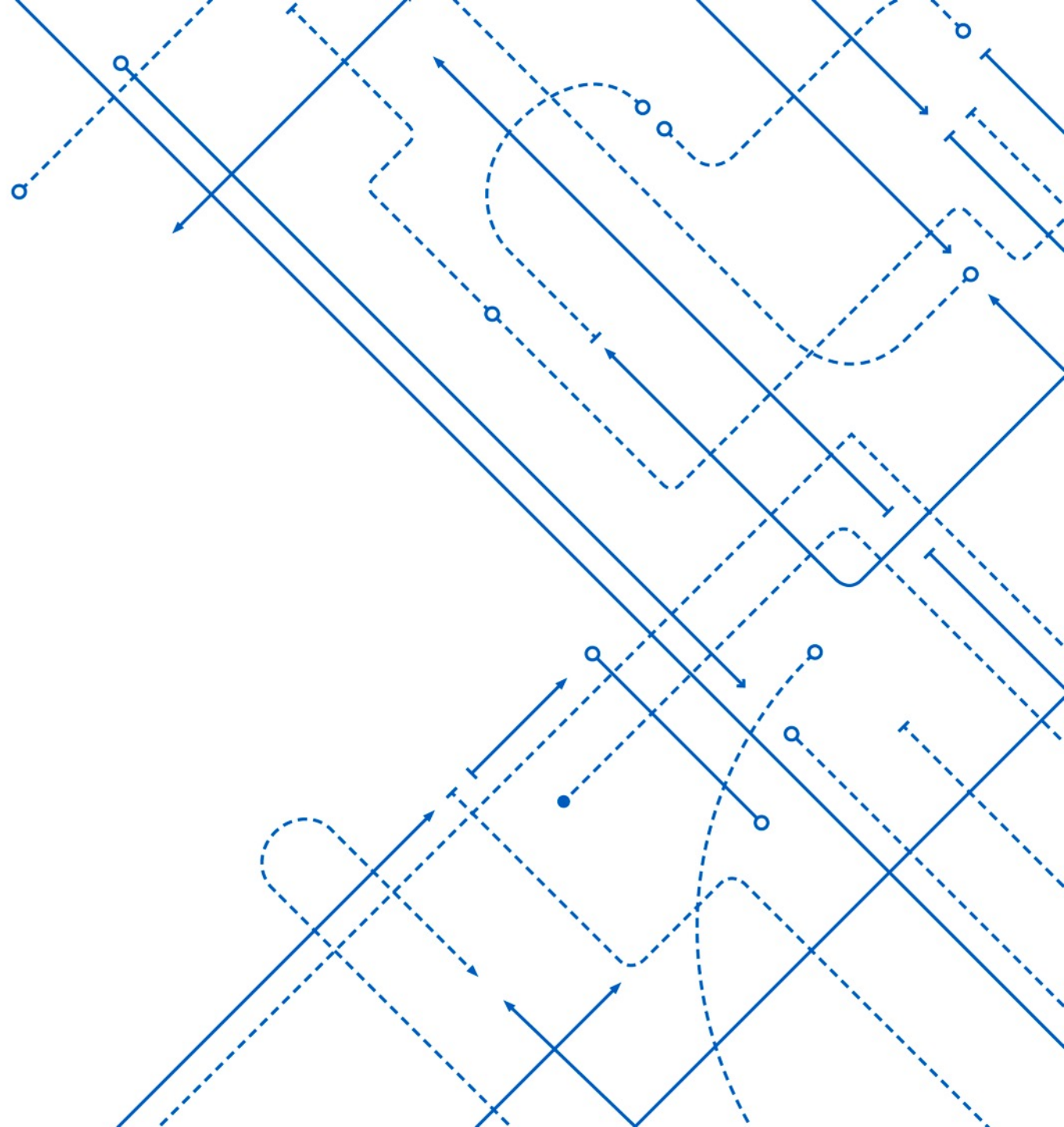
Risk & Compliance examples

- Policies, procedures, risk assessments, security plans, security-email-lists, investigations, HIPAA/PCI/FISMA/NIST/DUAs…, etc.



THE FOUR THINGS OF INFOSEC

Goals or principles



University at Buffalo
Information Technology

The Four Things (Goals) of Information Security

Keep the Bad Actors Out

- Edge firewall, controlled remote access and control, datacenter and network closet safeguards, SIEM & IDS/IPS…

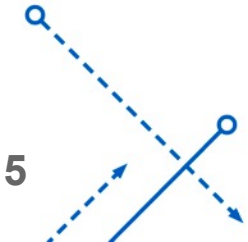
Verify the Trusts

- UBIDs and passwords, MultiFactor Authentication, SIEM & IDS/IPS (logging and alerts, impossible login detection, etc.)

Support creation and sharing of knowledge and information as intended

Keep UB safe by protecting our systems, data, and users

- Security standards, etc.



Summer 2019 Plans – IV Big Changes/Tools (see top 2 goals)

I. - Fully staff the ISO, improve the presence and communications (ISO Blog, etc.)

II. - Transition to SPLUNK

Logs and logging of all things needed (server security standards!)

Security dashboards, standard reports (Pivots: UBID -> IP -> UBIDs –> IPs ->Activities, etc.) (Impossible travel: login here and from Russia within 10 minutes of each other)

III. - NGFW Firewall tuning and changes – reduce attack surface (integration with Dept. Firewalls)

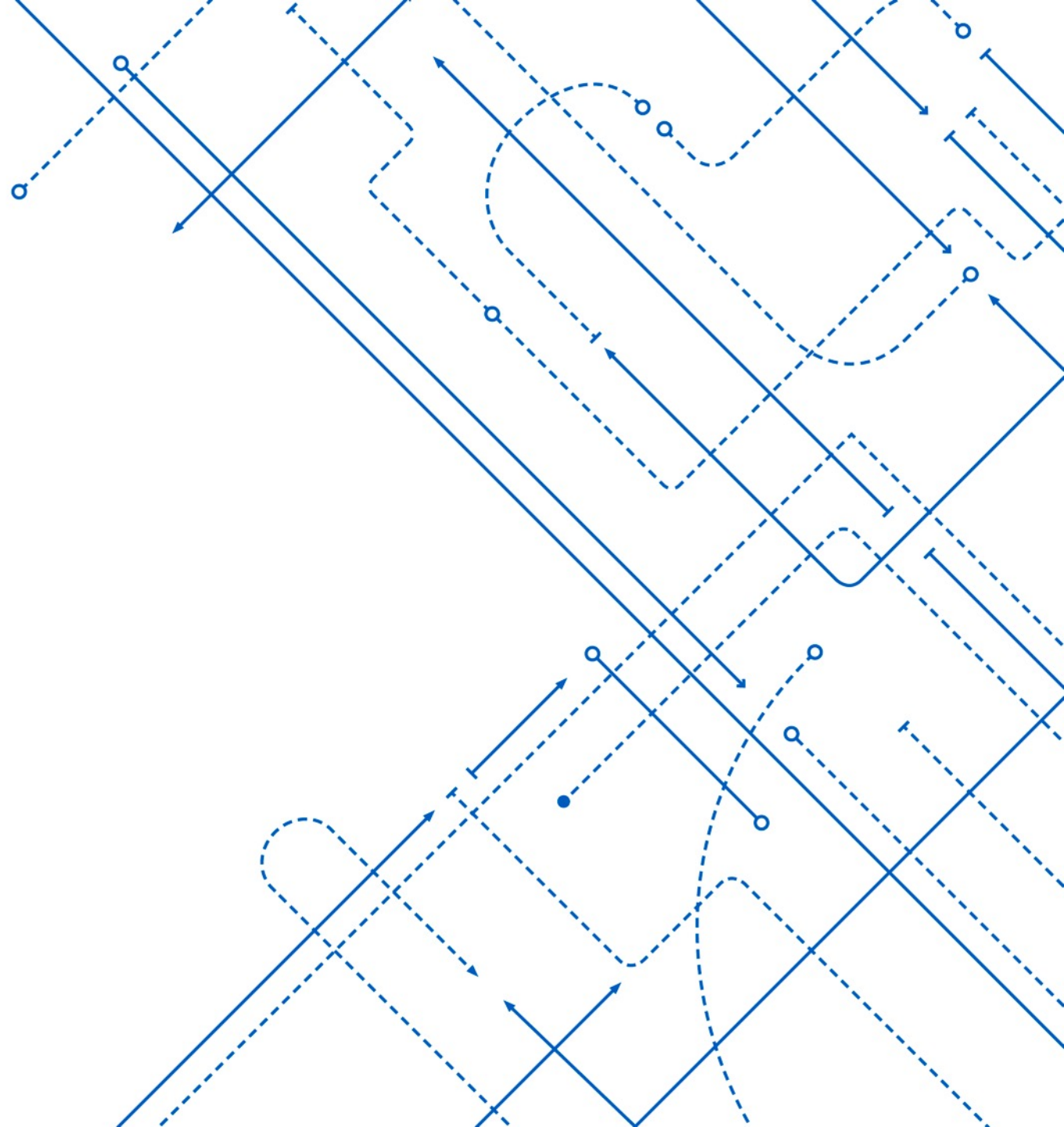
Control & Monitor Remote Access/Remote Control for attacks (RDP, SSH, etc.)

IV. - MFA??? (Next Fall opt-in, 2020 required (protect W2)? Students? Etc.)

Plus ongoing…Category 2 data and principles of protection (Minimum Necessary, Least Privilege…)

…Desktop Security Standard revisited and revisited…email controls/DLP?...

QUESTIONS?



University at Buffalo
Information Technology